HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH - VIỄN THÔNG
CƠ SỞ TP. HỒ CHÍ MINH

KỸ THUẬT MẠNG RIÊNG ẢO (VPN)

Biên soạn: THS. TRẦN CÔNG HÙNG

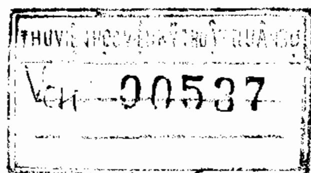
NHÀ XUẤT BẢN BƯU ĐIỆN
Tháng 7 - năm 2002

F988
CN
KY

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH - VIỄN THÔNG
CƠ SỞ TP. HỒ CHÍ MINH

KỸ THUẬT
MẠNG RIÊNG ẢO
(VPN)

Biên soạn: THS. TRẦN CÔNG HÙNG



NHÀ XUẤT BẢN BƯU ĐIỆN
Tháng 7 - năm 2002

LỜI TỰA

Các mạng viễn thông trước đây có đặc điểm chung là tồn tại một cách riêng lẻ, ứng với mỗi loại dịch vụ thông tin lại có ít nhất một loại mạng viễn thông riêng biệt để phục vụ dịch vụ đó. Mỗi mạng được thiết kế cho các dịch vụ riêng và không thể sử dụng cho các mục đích khác. Ví dụ ta không thể truyền thoại qua chuyển mạch gói X.25 vì trễ qua mạng này quá lớn.

Mỗi mạng lại yêu cầu phương pháp thiết kế, sản xuất, vận hành, bảo dưỡng khác nhau. Như vậy hệ thống mạng viễn thông sẽ có nhiều nhược điểm. trong đó quan trọng nhất là:

- Chỉ truyền được các dịch vụ độc lập tương ứng với từng mạng.
- Thiếu sự mềm dẻo: do khó thích nghi với các yêu cầu của các dịch vụ khác nhau trong tương lai.
- Kém hiệu quả trong việc bảo dưỡng vận hành, cũng như sử dụng tài nguyên. Tài nguyên có sẵn trong mạng không thể chia sẻ cho các mạng khác cùng sử dụng.

Do vậy, yêu cầu có một mạng viễn thông duy nhất ngày càng trở nên bức thiết. Chúng ta có thể xét các nguyên nhân sau:

- Các yêu cầu về dịch vụ băng rộng tăng lên.
- Các yêu cầu kỹ thuật xử lý tín hiệu, chuyển mạch, truyền dẫn ở tốc độ cao (cỡ vài trăm Mbit/giây đến vài Gbit/giây) đã trở thành hiện thực.
- Sự cần thiết phải tổ hợp các dịch vụ phụ thuộc lẫn nhau ở chuyển mạch kênh và chuyển mạch gói vào một mạng băng rộng duy nhất.
- Sự cần thiết phải thoả mãn tính mềm dẻo cho các yêu cầu về phía người sử dụng cũng như người quản trị mạng.

Theo khuyến nghị ITU-T I.121 đưa ra mạng tổ hợp dịch vụ số băng rộng B-ISDN (Broadband Integrated Service Digital Network) cung cấp các cuộc nối trong B-ISDN phục vụ cho tất cả các dịch vụ chuyển mạch kênh, chuyển mạch

gói theo kiểu đa phương tiện, đơn phương tiện, theo kiểu hướng liên kết hoặc không liên kết. Mà theo ITU-T thì B-ISDN hoạt động dựa trên cơ sở phương thức truyền không đồng bộ ATM (Asynchronous Transfer Mode) như vậy ATM là nền tảng của B-ISDN.

Hiện nay thì công nghệ ATM vẫn chưa được đưa ra áp dụng ở Việt Nam, vẫn còn đang thử nghiệm, theo tôi được biết thì đã có nhiều nước đã áp dụng vào thực tế. Hiện nay thì các ứng dụng chuyển mạch nhãn đa giao thức MPLS (Multi-Protocol Label Switching) cũng được đưa ra và sử dụng ở Hàn Quốc. Công nghệ hệ thống MPLS là sự phối hợp giữa công nghệ chuyển mạch tốc độ cao ATM và công nghệ định tuyến IP. Đó là sự kết hợp các đặc tính của cả lớp 2 đầy đủ đến mạng lõi tốc độ cao và lớp 3 thích hợp cho chất lượng dịch vụ QoS. Các dịch vụ ứng dụng MPLS mở đường cho Internet thế hệ sau. Tuy nhiên sự tồn tại của MPLS thì không thể không nói đến sự tồn tại của mạng riêng ảo VPN (Virtual Private Network), vì MPLS dựa vào dịch vụ IP-VPN được phát triển như chức năng ứng dụng chính của hệ thống MPLS và hỗ trợ dịch vụ bởi sự kết nối các vị trí VPN dùng đường dẫn nhãn chuyển mạch MPLS LSP (MPLS Label Switched Path). Do đó để giúp cho sinh viên và các bạn ham thích về lĩnh vực viễn thông nói chung và hệ thống mạng số liệu nói riêng cụ thể nhất là công nghệ hệ thống MPLS trong tương lai ở nước ta, quyển sách này sẽ trang bị kiến thức về mạng riêng ảo (VPN), đó là một phần kiến thức cơ sở MPLS cho các bạn.

Tuy nhiên lần xuất bản đầu tiên không thể tránh khỏi những sai sót, tôi rất mong nhận được sự góp ý của quý độc giả để cuốn sách hoàn chỉnh hơn trong lần tái bản sau, mọi đóng góp xin gửi đến e-mail: conghung@ptithcm.edu.vn.

Xin chân thành cảm ơn.

Tác giả: THS. TRẦN CÔNG HÙNG

PHẦN MỞ ĐẦU

GIỚI THIỆU TỔNG QUAN VỀ VPN

Cụm từ Virtual Private Network hay tạm dịch là mạng riêng ảo, thường gọi tắt là VPN, thực sự bùng nổ vào năm 1997 và càng ngày càng có nhiều nhà cung cấp đưa ra những giải pháp riêng về VPN cho những khách hàng của họ, trên các tạp chí chuyên đề, trên Internet, ở đâu chúng ta cũng có thể bắt gặp những bài báo, những hội thảo liên quan đến VPN cũng như các sản phẩm hỗ trợ cho VPN. Trong quyển sách này chúng ta không thể đề cập hết đến mọi vấn đề thuộc VPN, tuy nhiên chúng ta sẽ đề cập đến những gì căn bản nhất của VPN cũng như cơ sở trong việc xây dựng một VPN cho một tổ chức, cơ quan,... Và trong phần giới thiệu này chúng ta sẽ xem xét đến những vấn đề cơ bản về VPN, các loại hình VPN, những lợi ích mà nó đem lại, cùng với một số vấn đề có liên quan.

1. Căn bản về mạng riêng ảo

Khái niệm về mạng riêng ảo

Mạng riêng ảo là phương pháp làm cho một mạng công cộng (ví dụ như mạng Internet) hoạt động giống như một mạng cục bộ, có cùng các đặc tính như bảo mật và tính ưu tiên mà người dùng từng ưa thích. VPN cho phép thành lập các kết nối riêng với những người dùng ở xa, các văn phòng chi nhánh của công ty và đối tác của công ty đang sử dụng chung một mạng công cộng. Mạng diện rộng WAN (Wide Area Network) truyền thống yêu cầu công ty phải trả chi phí và duy trì nhiều loại đường dây riêng, song song với việc đầu tư các thiết bị và đội ngũ cán bộ. Nhưng những vấn đề về chi phí làm cho các công ty dù muốn hưởng những lợi ích mà việc mở rộng mạng đem lại nhưng đôi khi họ không thực hiện nổi. Trong khi đó, VPN không bị những rào cản về chi phí như các mạng WAN trên do được thực hiện qua một mạng công cộng.

Thực ra, khái niệm VPN không phải là một công nghệ mới, chúng đã từng được sử dụng trong các mạng điện thoại (Telephone Networks) cách đây một vài năm và trở nên phổ biến do sự phát triển của mạng thông minh. Các mạng VPN chỉ trở nên thực sự có tính mới mẻ khi chúng chuyển thành các mạng IP (mạng sử dụng giao thức Internet) chẳng hạn như mạng Internet. Do đó, nhiều người đã dùng thuật ngữ Internet VPN và mạng dữ liệu riêng ảo VPDN (Virtual Private Data Network) để thay cho thuật ngữ VPN. VPN sử dụng việc mã hoá dữ liệu để ngăn ngừa các người dùng không được phép truy cập đến dữ liệu và bảo đảm dữ liệu không bị sửa đổi.

Định đường hầm (tunneling) là một cơ chế dùng cho việc đóng gói (encapsulate) một giao thức vào trong một giao thức khác. Trong ngữ cảnh Internet, định đường hầm cho phép những giao thức như IPX, AppleTalk và IP được mã hoá, sau đó đóng gói trong IP. Tương tự, trong ngữ cảnh VPN, định đường hầm che giấu giao thức lớp mạng nguyên thủy bằng cách mã hoá gói dữ liệu và chứa gói đã mã hoá vào trong một vỏ bọc IP (IP envelope). Vỏ bọc IP này, thực ra là một gói IP, sau đó sẽ được chuyển đi một cách bảo mật qua mạng Internet. Tại bên nhận, sau khi nhận được gói trên sẽ tiến hành gỡ bỏ vỏ bọc bên ngoài và giải mã thông tin dữ liệu trong gói này và phân phối đến thiết bị truy cập thích hợp, chẳng hạn như một bộ định tuyến.

VPN còn cung cấp các thoả thuận về chất lượng dịch vụ (QoS), những thoả thuận này thường được định ra cho một giới hạn trên cho phép về độ trễ trung bình của gói trong mạng. Ngoài ra, các thoả thuận trên có thể kèm theo một sự chỉ định cho giới hạn dưới của băng thông hiệu dụng cho mỗi người dùng. Các thoả thuận này được phát triển thông qua các thoả thuận mức dịch vụ SLA (Service Level Agreements) với nhà cung cấp dịch vụ. Chúng ta sẽ đề cập chi tiết hơn về các thoả thuận SLA này ở phần sau.

Qua những vấn đề đã trình bày như trên, có thể định nghĩa VPN một cách ngắn gọn qua công thức sau:

VPN = Định đường hầm + Bảo mật + Các thỏa thuận về QoS

Nhờ vào lợi thế của các ứng dụng quan trọng được triển khai trên mạng Intranet và các mạng truy cập từ xa đã làm cho khách hàng thỏa mãn hơn trong công việc của họ, hoạt động kinh doanh của công ty trở nên hợp lý, hiệu quả và đạt tới những thị trường rộng lớn hơn. Tuy nhiên các vấn đề về chi phí mạng (bao gồm chi phí thiết bị, đường dây, chi phí cho việc bảo dưỡng,...) cũng như việc quản lý mạng là những vấn đề quan trọng đối với nhiều công ty, đặc biệt là những công ty muốn thu hồi vốn nhanh để tái sản xuất. Do đó người ta đã đưa ra giải pháp xây dựng những mạng riêng ảo để giảm thiểu chi phí mạng cho công ty, thay thế cho các giải pháp dùng đường truyền chuyên biệt truyền thống như trước đây.

Nhờ vào việc nối mạng qua VPN tiết kiệm chi phí hơn hẳn giải pháp thuê bao đường truyền, các doanh nghiệp có thể tự mình mở rộng tầm hoạt động của công ty ở mức toàn cầu (thông qua mạng Internet) mà không cần đầu tư ở mức qui mô toàn cầu! VPN có vai trò quan trọng trong doanh nghiệp nhờ vào việc giảm chi phí kết nối đối với các nhân viên lưu động (mobile worker) - vì các công ty có nhiều chi nhánh trên thế giới thì đội ngũ nhân viên của họ rất đông, nhiều người phải làm việc ở những quốc gia xa với trung tâm - mở rộng Intranet đến các văn phòng chi nhánh, liên lạc với đối tác và khách hàng chủ yếu thông qua mạng Extranet. Sau đây sẽ đề cập đến một số lợi ích, giá trị của VPN, các thuật ngữ liên quan đến VPN, cũng như trình bày tổng quát các phương thức hoạt động hiện nay của các VPN, để tạo điều kiện cho việc lựa chọn phương thức thích hợp, hiệu quả nhất để xây dựng một VPN.

Những lợi ích do VPN đem lại

VPN mang lại lợi ích thực sự và tức thời cho công ty. Có thể dùng VPN để đơn giản hoá việc truy cập đối với các nhân viên làm việc và người dùng lưu động, mở rộng Intranet đến từng văn phòng chi nhánh, thậm chí triển khai Extranet đến tận khách hàng và các đối tác chủ chốt và điều quan trọng là những công việc trên đều có chi phí thấp hơn nhiều so với việc mua thiết bị và đường dây cho mạng WAN riêng. VPN do một nhà cung cấp dịch vụ làm chủ và quản lý, bằng quy mô kinh tế và các công nghệ tiên tiến, họ có thể phục vụ nhiều tổ chức trên cùng một mạng, dùng các phần mềm hiện đại để phân biệt lưu lượng dữ liệu của công ty này được tách riêng với các công ty khác. Có thể dẫn chứng những ưu điểm của VPN như sau:

Giảm chi phí thường xuyên: VPN cho phép tiết kiệm đến 60% chi phí so với thuê đường truyền và giảm đáng kể tiền cước gọi đến của các nhân viên làm việc ở xa. Giảm được cước phí đường dài khi truy cập VPN cho các nhân viên di động và các nhân viên làm việc ở xa nhờ vào việc họ truy nhập vào mạng thông qua các điểm kết nối POP (Point of Presence) ở địa phương, hạn chế gọi đường dài đến các modem tập trung.

Giảm chi phí đầu tư: Sẽ không tốn chi phí đầu tư cho máy chủ, bộ định tuyến cho mạng đường trục và các bộ chuyển mạch phục vụ cho việc truy cập bởi vì các thiết bị này do các nhà cung cấp dịch vụ quản lý và làm chủ. Công ty cũng không phải mua, thiết lập cấu hình hoặc quản lý các nhóm modem phức tạp. Ngoài ra họ cũng có thể thuê với giá rẻ các thiết bị phục vụ khách hàng, thường có sẵn ở các nhà cung cấp dịch vụ, hoặc từ các công ty dịch vụ giá trị gia tăng, nhờ thế việc nâng cấp mạng cũng trở nên dễ dàng và ít tốn kém hơn.

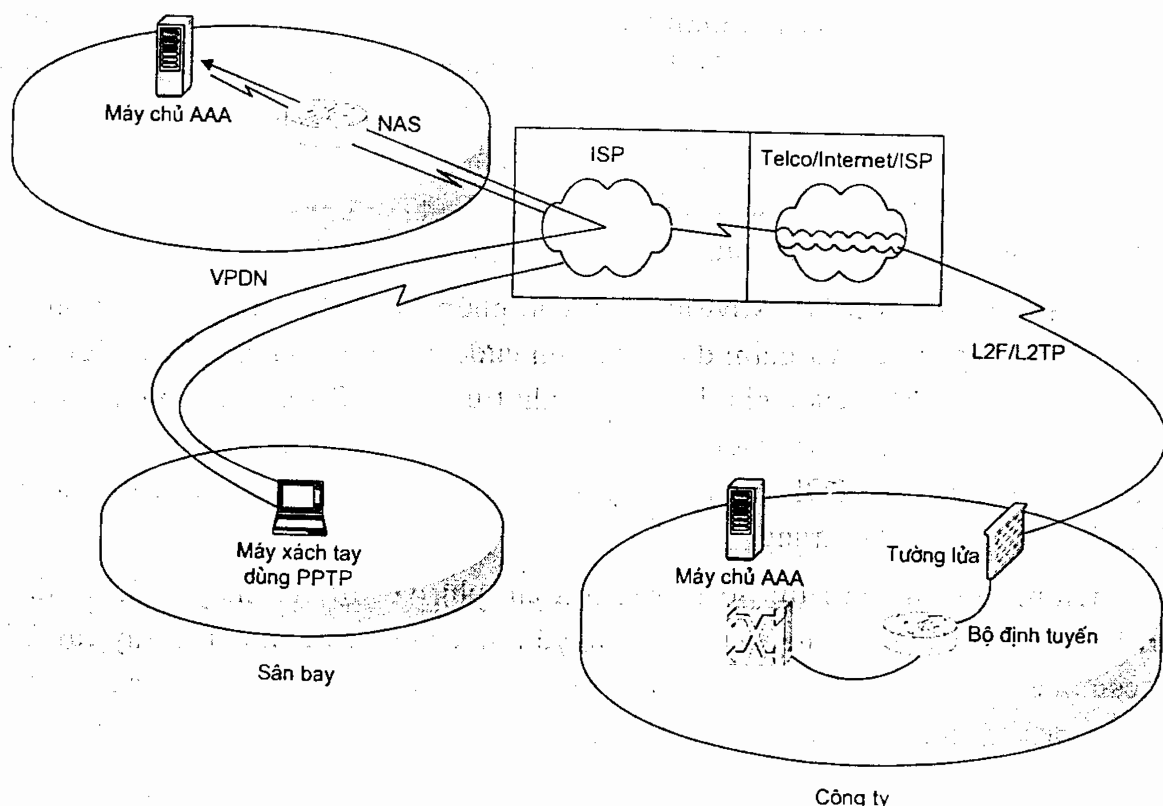
Giảm chi phí quản lý và hỗ trợ: Với quy mô kinh tế của mình, các nhà cung cấp dịch vụ có thể mang lại cho công ty những khoản tiết kiệm có giá trị so với việc tự quản lý mạng, giảm hay loại trừ hẳn yêu cầu nhân viên "tại nhà". Hơn nữa, nhận được sự hỗ trợ và phục vụ 24/24 do những nhân viên lành nghề luôn sẵn sàng đáp ứng mọi lúc, giải quyết nhanh chóng các sự cố.

Truy cập mọi lúc, mọi nơi: Khách hàng của VPN qua mạng mở rộng này, có cùng quyền truy cập và khả năng như nhau đối với các dịch vụ trung tâm bao gồm WWW, e-mail, FTP... cũng như các ứng dụng thiết yếu khác, khi truy cập chúng thông qua những phương tiện khác nhau như qua mạng cục bộ LAN (Local Area Network), modem, modem cáp, đường dây thuê bao số xDSL... mà không cần quan tâm đến những phần phức tạp bên dưới.

2. Các loại VPN

Hiện tại chúng ta có thể phân VPN ra làm ba loại như sau:

1. Các VPN truy cập từ xa (Remote Access VPN): các VPN này cung cấp truy cập tin cậy cho những người dùng đầu xa như các nhân viên di động, các nhân viên ở xa và các văn phòng chi nhánh thuộc mạng lưới của công ty.

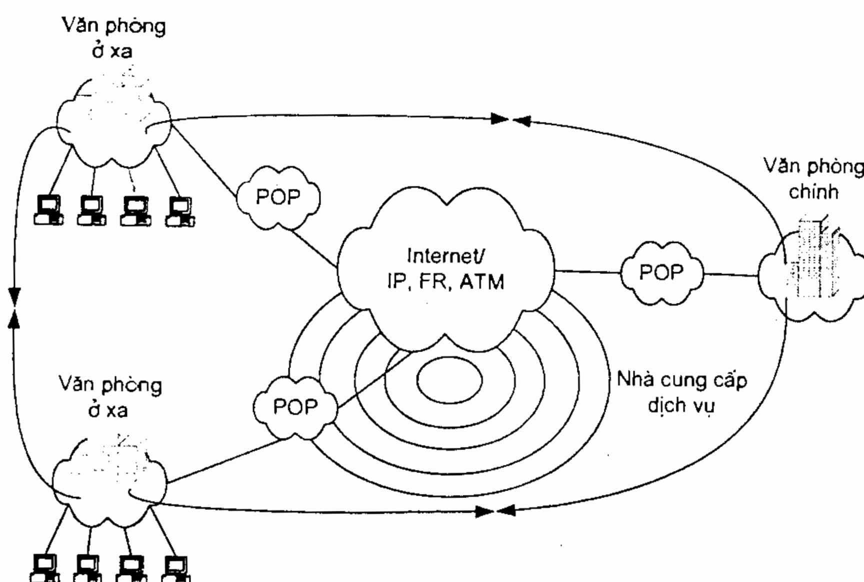


Hình 1: Các VPN truy cập từ xa

2. Các VPN nội bộ (Intranet VPN): chúng cho phép các văn phòng chi nhánh được liên kết một cách bảo mật đến trụ sở chính của công ty (hình 2).
3. Các VPN mở rộng (Extranet VPN): cho phép các khách hàng, các nhà cung cấp và các đối tác có thể truy cập một cách bảo mật đến mạng Intranet của công ty.

3. Cấu trúc của VPN

Tất cả các VPN đều cho phép truy cập bảo mật qua các mạng công cộng bằng cách sử dụng những dịch vụ bảo mật, bao gồm việc định đường hầm (tunneling) và các biện pháp mã hoá dữ liệu. Trong phần này sẽ giới thiệu về một số thuật ngữ, các sản phẩm và các công nghệ có liên quan đến VPN.



Hình 2: Các Intranet VPN

Tính bảo mật

Bảo mật là những gì làm cho VPN trở nên có tính "ảo" và "riêng". Để cạnh tranh và nhiều lý do khác, việc bảo mật thông tin và các quá trình trao đổi thông tin của công ty trở nên có tính chất sống còn, đó là nguyên nhân các giải pháp WAN và đường truyền kênh thuê riêng được sử dụng một cách phổ biến như hiện nay. Như vậy, yêu cầu của VPN là phải bảo mật như đường dây thuê riêng, đồng thời mang lại những ưu điểm về chi phí mà không cần phải bỏ những tính riêng tư của mạng. Do đó, cần kết hợp các sản phẩm và công nghệ với nhau để đảm bảo bảo mật cho các kết nối VPN.

Đường hầm

Các đường hầm (tunnel) chính là đặc tính ảo của VPN, nó làm cho một kết nối dường như một dòng lưu lượng duy nhất trên đường dây. Đồng thời còn tạo cho VPN khả năng duy trì những yêu cầu về bảo mật và quyền ưu tiên như đã được áp dụng trong mạng nội bộ, bảo đảm cho vai trò kiểm soát dòng lưu chuyển dữ liệu. Đường hầm cũng làm cho VPN có tính riêng tư.

Các loại công nghệ đường hầm được dùng phổ biến cho truy cập VPN gồm có giao thức định đường hầm điểm-điểm PPTP (Point to Point Tunneling Protocol), chuyển tiếp lớp 2 - L2F (Layer 2 Forwarding) hoặc giao thức định đường hầm lớp 2 - L2TP (Layer 2 Tunneling Protocol). Các mạng VPN nội bộ và mở rộng dành riêng có thể sử dụng những công nghệ như bảo mật IP - IPSec (IP security) hoặc bọc gói định tuyến chung GRE (Generic Route Encapsulation) để tạo nên các đường hầm ảo thường trực.

Mã hoá

Mã hoá (encryption) là tính năng tùy chọn nó cũng đóng góp vào đặc điểm "riêng tư" của VPN. Chỉ nên sử dụng mã hoá cho những dòng dữ liệu quan trọng đặc biệt, còn bình thường thì không cần vì việc mã hoá có thể ảnh hưởng xấu đến tốc độ, tăng gánh nặng cho bộ xử lý.

Tường lửa

Chúng ta sử dụng tường lửa (firewall) để bảo mật mạng nội bộ của mình chống lại những cuộc tấn công vào lưu lượng trên mạng và những kẻ phá hoại, giải pháp bức tường lửa tốt là công cụ có khả năng phân biệt các lưu lượng dựa trên cơ sở người dùng, trình ứng dụng hay nguồn gốc. Tường lửa sẽ được nói kỹ hơn trong phần II "Xây dựng các khối của một VPN"

Định danh người dùng (User Identification)

Mọi người dùng đều phải chịu sự kiểm tra xác thực để báo cho mạng biết thông tin về họ (quyền truy cập, mật khẩu, ...) và phải chịu sự ủy quyền để báo cho biết về những gì mà họ được phép làm. Một hệ thống tốt còn thực hiện tính toán để theo dõi những việc mà người dùng đã làm nhằm mục đích tính cước và bảo mật. Xác thực (Authentication), trao quyền (Athorization) và tính cước (Accounting) được gọi là các dịch vụ AAA.

Tính ưu tiên

Ưu tiên là quá trình "gán thẻ" cho dòng lưu lượng của một ứng dụng nào đó đối với các dịch vụ được xúc tiến thông qua mạng. Ví dụ như lưu thông các trình

ứng dụng nghiệp vụ quan trọng (chẳng hạn như các ứng dụng cơ sở dữ liệu danh mục hoặc bán hàng) có thể nhận được ưu tiên hàng đầu để chuyển nhanh, phù hợp với xu thế cạnh tranh trên thương trường, trong khi các dịch vụ như gửi e-mail hay truyền tập tin thì có ưu tiên thấp hơn. Khả năng gán quyền ưu tiên sẽ phải độc lập với dữ liệu truyền để đảm bảo tính hoàn hảo thực sự của dịch vụ.

4. Sơ lược về các giao thức dùng cho VPN

Hiện nay có ba giao thức chính dùng để xây dựng VPN là:

Giao thức định đường hầm điểm-điểm PPTP

Đây là giao thức định đường hầm phổ biến nhất hiện nay, PPTP (Point-to-Point Tunneling Protocol) được cung cấp như một phần của các dịch vụ truy cập từ xa RAS (Remote Access Services) trong hệ điều hành Microsoft Windows NT 4.0 và Windows 2000, sử dụng cách mã hoá sẵn có của Windows, xác thực người dùng và cơ sở cấu hình của giao thức điểm-điểm PPP (Point-to-Point Protocol) để thiết lập các khoá mã.

Giao thức định đường hầm lớp 2 - L2TP

Đây là giao thức chuẩn của IETF (Internet Enginneering Task Force) sử dụng kỹ thuật khoá công cộng (public key technology) để thực hiện việc xác thực người dùng và có thể hoạt động thông qua một môi trường truyền thông đa dạng hơn so với PPTP. Một điểm đáng lưu ý là L2TP (Layer 2 Tunneling Protocol) không thể sử dụng để thực hiện việc mã hoá. Microsoft bắt đầu cung cấp L2TP như một phần của RAS trong hệ điều hành Windows 2000.

Giao thức bảo mật IP - IPSec

Đây là một giao thức chuẩn của IETF dùng để cung cấp việc mã hoá. Lợi điểm lớn nhất của IPSec (IP Security) là giao thức này có thể được sử dụng để thiết lập một VPN một cách tự động và thích hợp với chính sách bảo mật tập trung và có thể sử dụng để thiết lập một VPN dựa trên cơ sở các máy tính mà không phải là các người dùng. IPSec được cung cấp như một phần trong hệ điều hành Windows NT 4.0 và Windows 2000.

Ngoài ra còn giao thức chuyển tiếp lớp 2 L2F (Layer 2 Forwarding) là cơ sở để xây dựng nên L2TP.

Để xây dựng một VPN bảo mật, chúng ta có thể dùng hai cách như sau:

Cách 1: Có thể dùng PPTP một cách độc lập vì bản thân PPTP có thể cung cấp một VPN bảo mật. Dùng cách này ta sẽ giảm thiểu được chi phí và việc quản lý sẽ ít phức tạp.

Cách 2: Kết hợp giữa L2TP và IPSec để cung cấp một VPN bảo mật, cách này thích hợp cho những công ty đòi hỏi tính bảo mật mạng cao, mặc dù phương pháp này sẽ gây tốn kém và việc quản lý mạng sẽ có độ phức tạp hơn so với cách trên.

5. Đánh giá chung về VPN

Tóm lại, với chi phí thỏa đáng, VPN có thể giúp doanh nghiệp tiếp xúc toàn cầu nhanh chóng và hiệu quả hơn về chi phí so với các giải pháp mạng diện rộng WAN khác. Ta có thể giảm chi phí thường xuyên một cách đáng kể và thu hồi vốn nhanh chóng Với VPN, chúng ta có thể mở rộng các trình ứng dụng nghiệp vụ tối quan trọng đến các văn phòng ở xa và các đối tác WAN khác qua Extranet, làm cho doanh nghiệp của mình có tính cạnh tranh mạnh hơn, đồng thời cũng cải thiện khả năng phục vụ khách hàng tốt hơn.

Ngày nay, trong nền kinh tế nối mạng tiến bộ nhanh chóng, một mô hình mới dùng cho truyền thông thương mại đã xuất hiện. Trong mô hình mới này, các nhà cung cấp dịch vụ hợp tác với khách hàng để phân phối các dịch vụ mạng, là nền tảng cho các hoạt động kinh doanh của họ và để nâng cao hiệu quả cạnh tranh. Mạng riêng ảo (VPN) đã thể hiện sự đột phá công nghệ, làm chuyển biến ngành công nghiệp và cách mạng hoá các dịch vụ do khách hàng yêu cầu. Mô hình mạng này hiện đang chuyển nhu cầu tự động hoá việc điều hành thông tin liên lạc riêng của các công ty sang quan hệ hợp tác với nhà cung cấp dịch vụ thông qua VPN để phát triển mạng của họ ra quy mô toàn cầu. Sự chuyển dịch nền móng mang tính chiến lược này đã mở ra những tiền đề thuận lợi để tiếp tục phát triển, khả năng thu lợi ngày càng nhiều và đạt hiệu quả cao nhất cho các nhà cung cấp dịch vụ lẫn khách hàng.

PHẦN I

VPN VÀ BẢO MẬT INTERNET VPN

CHƯƠNG 1

GIỚI THIỆU CHUNG

Kể từ khi những nhà kinh doanh bắt đầu sử dụng những chiếc máy tính tại nhiều vị trí, họ có mong muốn và nhu cầu kết nối những máy tính này lại với nhau trong một kiểu riêng và bảo mật nhằm dễ dàng cho việc thông tin liên lạc. Việc xây dựng một mạng riêng trên một khu vực nội bộ của những tòa nhà văn phòng có thể tương đối đơn giản, bởi vì các công ty thường có kiến trúc vật lý riêng. Nhưng mọi việc sẽ trở nên khó khăn hơn nhiều khi xây dựng một mạng chung bao gồm những văn phòng khác nhau hay các kiến trúc cách nhau rất xa tại các nước hay các bang khác nhau. Trong nhiều trường hợp, các nhà kinh doanh không có một sự lựa chọn nào khác ngoài việc sử dụng một kênh thuê riêng (leased line) từ tổng đài nội hạt của họ hay dùng những phương tiện khoảng cách xa để kết nối những máy tính ở các vị trí địa lý phân biệt (site) lại với nhau.

Các nhà kinh doanh từ lâu đã có nhiều cách để nối kết các địa điểm của họ hình thành những mạng kết hợp riêng (private corporate network). Nhưng cho đến gần đây, những mạng này trở nên cứng nhắc về bản chất (hard-wired), ít tính mềm dẻo. Sau khi các dịch vụ mạng được cung cấp để kết nối những site trên cơ sở chia sẻ các kết nối công cộng, thuật ngữ "mạng riêng ảo" hay VPN (Virtual Private Network) trở nên quen thuộc. Từ "virtual" ở đây được thêm vào như một từ bổ nghĩa để chỉ ra rằng mặc dù chúng ta có thể xem dòng lưu lượng giữa hai site như một kênh riêng, nhưng thật ra nó không được gắn cứng và tồn tại như một kết nối

khi lưu lượng mạng (traffic) chuyển qua trên kênh. Đó là một kênh ảo (virtual circuit).

1.1 Thế nào là một mạng Internet VPN?

Một mạng riêng ảo dựa trên Internet (Internet-based VPN) dùng cơ sở hạ tầng mở và phân tán của Internet cho việc truyền dữ liệu giữa các site của các công ty (corporate site). Về bản chất, những công ty sử dụng Internet VPN thiết lập các kết nối đến các điểm kết nối cục bộ của nhà cung cấp dịch vụ Internet ISP (Internet Service Provider), gọi là POP (Point of Presence) và để cho ISP bảo đảm rằng dữ liệu được truyền đến đích thông qua Internet.

Kết nối được tạo ra để hỗ trợ cho một phiên thông tin giữa các site được hình thành một cách linh động, nhằm giảm tải cho mạng, nên không có những kết nối thường trực trong cấu trúc của Internet VPN. Nói một cách khác, băng thông yêu cầu cho một phiên làm việc không được chỉ định cho đến khi nó được yêu cầu và được giải phóng khi một phiên làm việc kết thúc. Trong nhiều cách thì khía cạnh này tương tự với tính chất của mạng chuyển tiếp khung (Frame Relay), nhưng nó được mở rộng thành nhiều kiểu kết nối khác trên Internet.

Bởi vì Internet là một mạng công cộng với việc truyền hầu hết dữ liệu mở Internet VPN bao gồm cung cấp cơ chế mã hoá dữ liệu truyền giữa các site VPN, nhằm bảo mật dữ liệu chống lại nghe trộm (sniffing) và can thiệp (tampering) từ những thành viên bất hợp pháp (unauthorized parties).

Với lợi điểm thêm vào này, Internet VPN cũng cung cấp kết nối bảo mật cho những đối tượng di động (mobile worker) bởi đặc tính của việc đánh số các kết nối quay số mà các ISP cung cấp cho các client (khách hàng) tại các POP của họ.

1.2 Các ưu điểm của một Internet VPN

Một số lợi ích xuất hiện từ việc sử dụng VPN dựa trên Internet cho dù việc xây dựng mạng VPN từ đầu hay việc chuyển mạng VPN truyền thống thành mạng VPN sử dụng Internet. Những lợi ích này dù trực tiếp hay gián tiếp bao gồm: tiết kiệm chi phí (cost saving), tính mềm dẻo (flexibility), khả năng mở rộng (scalability) và một số ưu điểm khác.

1.2.1 Chi phí thấp

Qua các bảng 1.1, 1.2, 1.3, chúng ta có thể so sánh chi phí khi sử dụng đường kênh thuê riêng T1 (1.5 Mbit/s) với chi phí khi sử dụng Internet VPN.

PHẦN I

VPN VÀ BẢO MẬT INTERNET VPN

CHƯƠNG 1

GIỚI THIỆU CHUNG

Kể từ khi những nhà kinh doanh bắt đầu sử dụng những chiếc máy tính tại nhiều vị trí, họ có mong muốn và nhu cầu kết nối những máy tính này lại với nhau trong một kiểu riêng và bảo mật nhằm dễ dàng cho việc thông tin liên lạc. Việc xây dựng một mạng riêng trên một khu vực nội bộ của những tòa nhà văn phòng có thể tương đối đơn giản, bởi vì các công ty thường có kiến trúc vật lý riêng. Nhưng mọi việc sẽ trở nên khó khăn hơn nhiều khi xây dựng một mạng chung bao gồm những văn phòng khác nhau hay các kiến trúc cách nhau rất xa tại các nước hay các bang khác nhau. Trong nhiều trường hợp, các nhà kinh doanh không có một sự lựa chọn nào khác ngoài việc sử dụng một kênh thuê riêng (leased line) từ tổng đài nột hạt của họ hay dùng những phương tiện khoảng cách xa để kết nối những máy tính ở các vị trí địa lý phân biệt (site) lại với nhau.

Các nhà kinh doanh từ lâu đã có nhiều cách để nối kết các địa điểm của họ hình thành những mạng kết hợp riêng (private corporate network). Nhưng cho đến gần đây, những mạng này trở nên cứng nhắc về bản chất (hard-wired), ít tính mềm dẻo. Sau khi các dịch vụ mạng được cung cấp để kết nối những site trên cơ sở chia sẻ các kết nối công cộng, thuật ngữ "mạng riêng ảo" hay VPN (Virtual Private Network) trở nên quen thuộc. Từ "virtual" ở đây được thêm vào như một từ bổ nghĩa để chỉ ra rằng mặc dù chúng ta có thể xem dòng lưu lượng giữa hai site như một kênh riêng, nhưng thật ra nó không được gắn cứng và tồn tại như một kết nối

khi lưu lượng mạng (traffic) chuyển qua trên kênh. Đó là một kênh ảo (virtual circuit).

1.1 Thế nào là một mạng Internet VPN?

Một mạng riêng ảo dựa trên Internet (Internet-based VPN) dùng cơ sở hạ tầng mở và phân tán của Internet cho việc truyền dữ liệu giữa các site của các công ty (corporate site). Về bản chất, những công ty sử dụng Internet VPN thiết lập các kết nối đến các điểm kết nối cục bộ của nhà cung cấp dịch vụ Internet ISP (Internet Service Provider), gọi là POP (Point of Presence) và để cho ISP bảo đảm rằng dữ liệu được truyền đến đích thông qua Internet.

Kết nối được tạo ra để hỗ trợ cho một phiên thông tin giữa các site được hình thành một cách linh động, nhằm giảm tải cho mạng, nên không có những kết nối thường trực trong cấu trúc của Internet VPN. Nói một cách khác, băng thông yêu cầu cho một phiên làm việc không được chỉ định cho đến khi nó được yêu cầu và được giải phóng khi một phiên làm việc kết thúc. Trong nhiều cách thì khía cạnh này tương tự với tính chất của mạng chuyển tiếp khung (Frame Relay), nhưng nó được mở rộng thành nhiều kiểu kết nối khác trên Internet.

Bởi vì Internet là một mạng công cộng với việc truyền hầu hết dữ liệu mở Internet VPN bao gồm cung cấp cơ chế mã hoá dữ liệu truyền giữa các site VPN, nhằm bảo mật dữ liệu chống lại nghe trộm (sniffing) và can thiệp (tampering) từ những thành viên bất hợp pháp (unauthorized parties).

Với lợi điểm thêm vào này, Internet VPN cũng cung cấp kết nối bảo mật cho những đối tượng di động (mobile worker) bởi đặc tính của việc đánh số các kết nối quay số mà các ISP cung cấp cho các client (khách hàng) tại các POP của họ.

1.2 Các ưu điểm của một Internet VPN

Một số lợi ích xuất hiện từ việc sử dụng VPN dựa trên Internet cho dù việc xây dựng mạng VPN từ đầu hay việc chuyển mạng VPN truyền thống thành mạng VPN sử dụng Internet. Những lợi ích này dù trực tiếp hay gián tiếp bao gồm: tiết kiệm chi phí (cost saving), tính mềm dẻo (flexibility), khả năng mở rộng (scalability) và một số ưu điểm khác.

1.2.1 Chi phí thấp

Qua các bảng 1.1, 1.2, 1.3, chúng ta có thể so sánh chi phí khi sử dụng đường kênh thuê riêng T1 (1.5 Mbit/s) với chi phí khi sử dụng Internet VPN.

Bảng1.1: Chi phí hàng tháng cho các mạng dùng đường kênh thuê riêng đơn so với Internet VPN

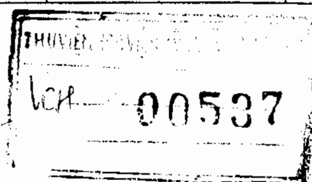
Thành phố	Khoảng cách (dặm)	Chi phí cho T1	Chi phí cho Internet VPN
Boston - New York	194	$4.570	$1.900
New York - Washington	235	$4.775	$1.900
Tổng		**$9.345**	**$3.800**

Bảng1.2: Chi phí hàng tháng cho các mạng mắt lưới kênh thuê riêng so với Internet VPN

Thành phố	Khoảng cách (dặm)	Chi phí cho T1	Chi phí cho Internet VPN
Boston - New York	194	$4.570	$1.900
New York -Washington	235	$4.775	$1.900
Boston - Wasington	463	$5.915	$1.900
Tổng		**$15.260**	**$5.700**

Bảng1.3: Chi phí hàng tháng cho các mạng dùng đường kênh thuê riêng kép so với Internet VPN

Thành phố	Khoảng cách (dặm)	Chi phí cho T1	Chi phí cho Internet VPN
San FranCisco - Denver	1.267	$13.535	$1.900
Denver - Chicago	1.023	$12.315	$1.900
Chicago - New York	807	$11.235	$1.900
San FranCisco - Los Angeles	384	$5.520	$1.900
Denver - Salt Lake	537	$6.285	$1.900
Denver - Dallas	794	$7.570	$1.900
Chicago - Minneapolis	410	$5.650	$1.900
New York - Wasington	235	$4.775	$1.900
New York - Boston	194	$4.570	$1.900
Tổng		**$71.455**	**$17.100**

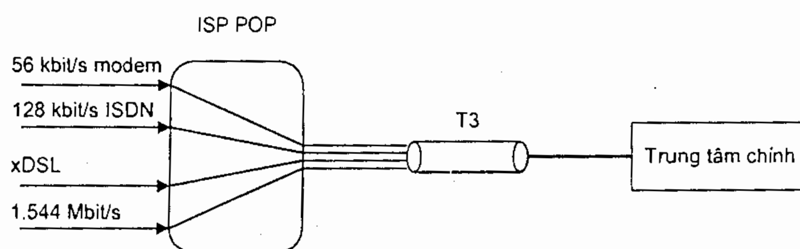


1.2.2 Tính mềm dẻo

Với các mạng VPN truyền thống, những kết nối dành cho các chi nhánh văn phòng nhỏ hơn, các máy tính từ xa với các phương tiện di động sử dụng xDSL, ISDN và những modem tốc độ cao, cần phải được duy trì với các thiết bị riêng (ví dụ như các dải modem) không thuộc phần cài đặt của các đường kênh thuê riêng hay thậm chí các mạng Frame Relay.

Trong mạng VPN dựa trên Internet, không chỉ T1 và T3 có thể được sử dụng giữa các văn phòng với ISP, mà nhiều kiểu kết nối khác cũng có thể được sử dụng để kết nối các văn phòng nhỏ và các đối tượng di động đến các ISP và do đó đến mạng riêng VPN. Điều hạn chế duy nhất là môi trường mà ISP hỗ trợ và số môi trường được cung cấp gia tăng một cách đều đặn.

Bởi vì những kết nối điểm-điểm (point-to-point) không phải là một thành phần của Internet VPN, cho nên không cần phải cung cấp môi trường và tốc độ giống nhau tại mỗi điểm (site), do đó làm giảm thiết bị và chi phí cung cấp.



ISP POP: Điểm kết nối cục bộ của nhà cung cấp dịch vụ Internet

Hình 1.1: Luồng lưu lượng đến hợp nhất

1.2.3 Khả năng mở rộng

Do VPN sử dụng môi trường và các công nghệ tương tự như Internet, cho nên nó có thể cung cấp cho những nhà kinh doanh hai hướng mở rộng mạng.

Trước tiên đó là về mặt địa lý. Với một Internet VPN, các văn phòng, nhóm và đối tượng di động có thể trở nên một phần của một mạng VPN ở bất kỳ nơi nào ISP cung cấp một điểm kết nối cục bộ POP. Hầu hết các ISP lớn đều có một số chỉ định các POP được trải rộng trên toàn nước Mỹ và Canada, trong đó có nhiều ISP cũng cung cấp các điểm POP ở Châu Âu và Châu Á. Khả năng mở rộng (scalability) cũng có thể linh động: một bộ phận văn phòng ở địa điểm của khách hàng có thể được kết nối một cách dễ dàng đến một POP nội bộ trong một vài phút (bằng cách sử dụng đường dây điện thoại thông thường và một modem)

và được gỡ ra dễ dàng khỏi mạng VPN khi văn phòng này bị đóng cửa, không còn hoạt động nữa. Dĩ nhiên, những kết nối đòi hỏi băng thông cao hơn phải mất nhiều thời gian hơn để thiết lập, nhưng dù vậy việc thiết lập cũng tương đối dễ dàng hơn khi thiết lập một đường kênh thuê riêng.

Thứ hai, đó là khả năng mở rộng băng thông. Chúng ta đã đề cập đến ISP thanh toán dựa trên việc sử dụng, vì thế chi phí cho một đường T1 sử dụng ít thì thấp hơn so với những chi phí cho một đường T1 sử dụng nhiều hơn. Nhưng các ISP cũng có thể nhanh chóng cung cấp một chọn lựa các độ rộng băng thông phù hợp với nhu cầu của các site. Ví dụ như một văn phòng chính có thể yêu cầu một đường T1 hay thậm chí một kết nối T3, trong khi các chi nhánh có thể liên lạc bằng một đường quay số (dial-up) dùng modem hay một đường ISDN. Và nếu như một văn phòng chi nhánh yêu cầu băng thông lớn hơn, thì nó có thể được nâng cấp dễ dàng từ một đường dây điện thoại lên đến 56 kbit/s hay từ kết nối ISDN lên kết nối bằng đường T1.

1.2.4 Giảm thiểu các hỗ trợ kỹ thuật

Việc chuẩn hoá trên một kiểu kết nối từ đối tượng di động (mobile worker) đến một POP của ISP và việc chuẩn hoá các yêu cầu về bảo mật đã làm giảm thiểu nhu cầu về nguồn hỗ trợ kỹ thuật cho mạng VPN. Và các nguồn xuất VPN cũng có thể làm giảm các yêu cầu hỗ trợ kỹ thuật bên trong khi các nhà cung cấp dịch vụ đảm nhiệm các nhiệm vụ hỗ trợ cho mạng.

1.2.5 Giảm thiểu các yêu cầu về thiết bị

Bằng việc cung cấp một giải pháp đơn cho các mạng xí nghiệp truy cập bằng quay số (dial-in) và truy cập Internet, Internet VPN yêu cầu về thiết bị ít hơn. Tốt hơn nhiều so với việc bảo trì các dải modem (modem bank) riêng biệt, các card tương thích (adapter) cho thiết bị đầu cuối và các máy chủ truy cập từ xa, một doanh nghiệp có thể thiết lập các thiết bị khách hàng CPE (Customer Premises Equipment) cho một môi trường đơn, như một đường T1, với phần còn lại của kết nối được thực hiện bởi ISP. Bộ phận IT có thể làm việc thiết lập kết nối WAN và duy trì bằng cách thay các dải modem và các mạch nhân của Frame Relay bằng một kết nối diện rộng đơn có thể đáp ứng lưu lượng của các người dùng từ xa, kết nối LAN-LAN và lưu lượng Internet cùng một lúc.

1.2.6 Đáp ứng các nhu cầu thương mại

Khi tích hợp nhiều công nghệ mới vào một mạng thương mại thì ta vẫn quan tâm đến các vấn đề như: chuẩn hoá, khả năng quản trị, khả năng mở rộng, khả năng tích hợp mang tính kế thừa, độ tin cậy và hiệu suất hoạt động.

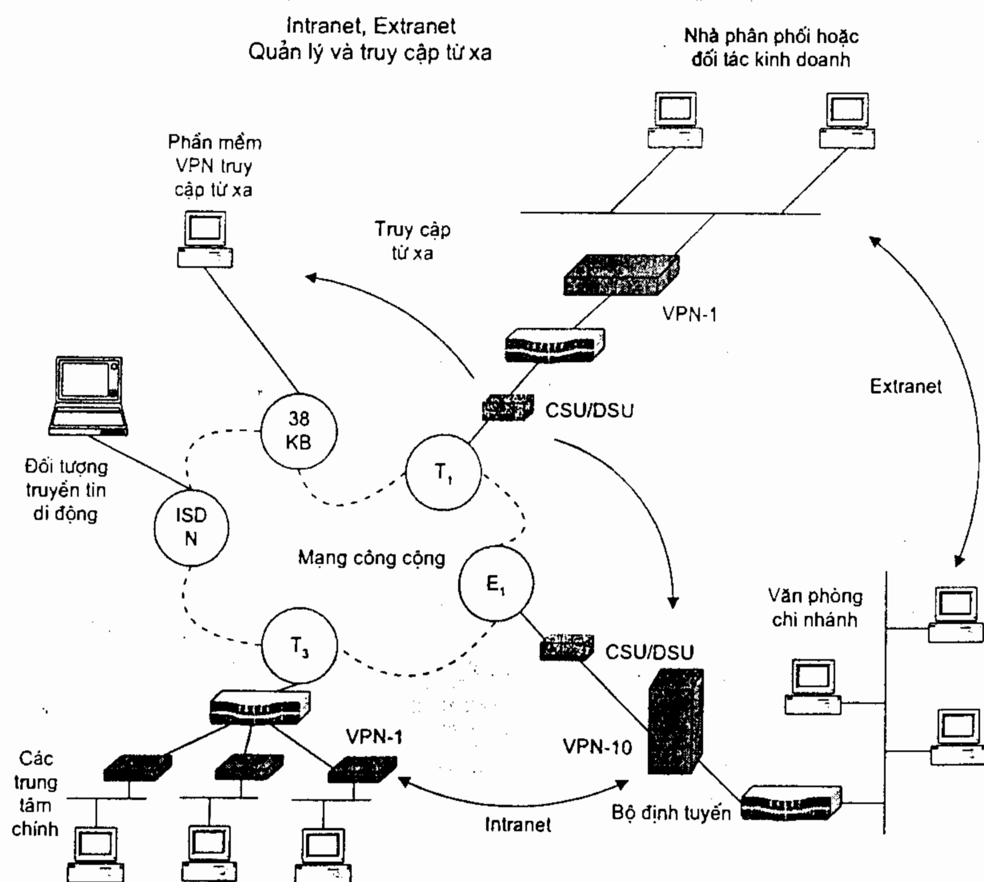
Các sản phẩm dịch vụ tuân theo các chuẩn chung hiện nay, một phần để đảm bảo tuổi thọ của sản phẩm nhưng có lẽ quan trọng hơn là sản phẩm từ nhiều nhà cung cấp khác có thể làm việc được với nhau. Ngay cả khi đấy, nhiều công ty vẫn chọn sản phẩm của một nhà cung cấp cho thiết bị mạng của họ, vì thế giảm được nhu cầu cho khả năng tương thích của các thiết bị, giảm được khả năng xung đột của các sản phẩm thuộc các nhà cung cấp khác nhau.

Vì mạng ngày càng trở nên phức tạp và số lượng người dùng ngày càng tăng, người quản trị mạng phải tìm cách để quản lý, giám sát và cấu hình các thiết bị mạng và phải thường xuyên thực hiện các công việc này cùng với số nhân viên ngày càng giảm vì hiếm khi mà thấy số lượng nhân viên tăng khi mạng tăng. Vì thế, khi thêm các dịch vụ hay thành phần mới nào vào mạng cần phải chú ý nó có thích hợp với hệ thống mạng hiện tại hay không, đặc biệt là bảo mật trong mạng VPN.

Người quản trị mạng phải lập kế hoạch dự báo cho sự phát triển của mạng, tránh sự thay đổi nhiều, khi nhu cầu về dịch vụ tăng.

CHƯƠNG 2

CÁC LOẠI MẠNG VPN

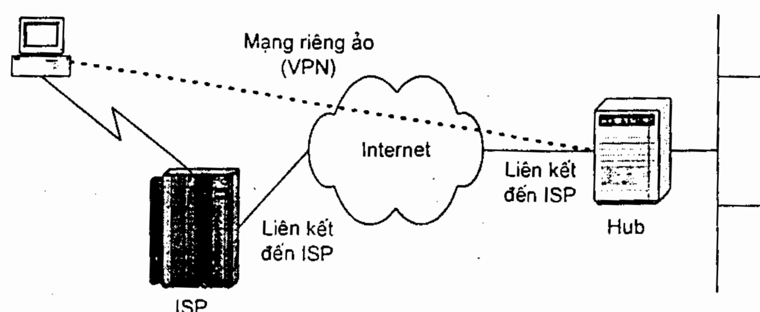


Hình 2.1: Các giải pháp VPN

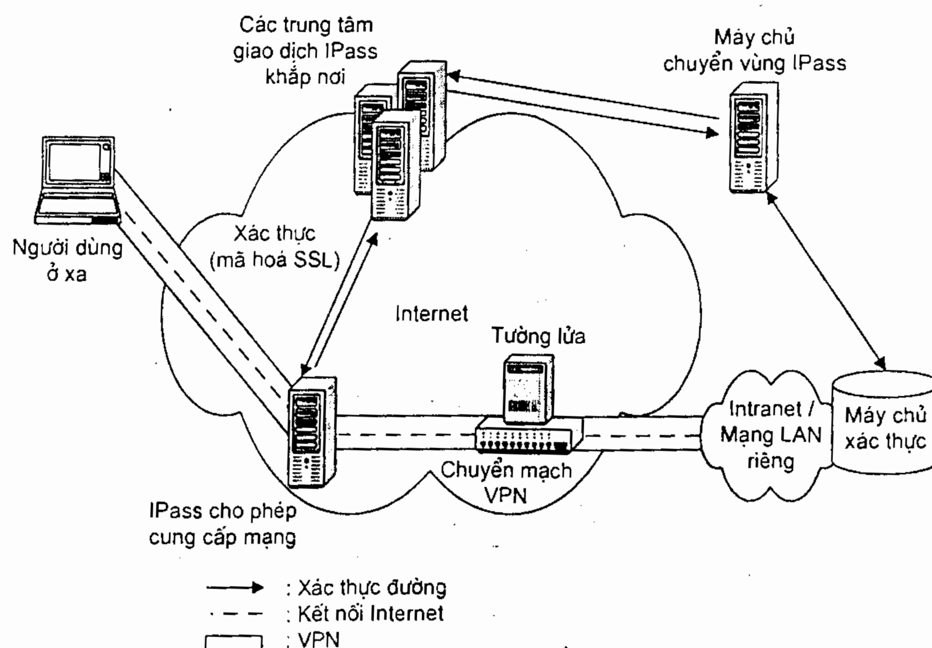
Có hai cách chủ yếu sử dụng các mạng riêng ảo VPN. Trước tiên, các mạng VPN có thể kết nối hai mạng với nhau. Điều này được biết đến như một mạng kết nối LAN-LAN VPN hay một mạng site-nối-site VPN. Thứ hai, một VPN truy cập từ xa có thể kết nối một người dùng từ xa với mạng.

2.1 Các người dùng truy cập từ xa thông qua Internet (Access VPN)

Cung cấp các truy cập từ xa đến một Intranet hay Extranet dựa trên cấu trúc hạ tầng chia sẻ Access VPN, người dùng có khả năng truy cập đến các tài nguyên trong VPN bất cứ khi nào, ở đâu mà nó cần. Đường truyền trong Access VPN có thể là tương tự, quay số, ISDN, các đường thuê bao số (DSL), IP di động và cáp để nối các người dùng di chuyển, máy tính từ xa hay các văn phòng lại với nhau. Ví dụ minh hoạ trên hình 2.3.



Hình 2.2: Dùng VPN dể kết nối client từ xa đến mạng LAN riêng



Hình 2.3: Tổ chức truy cập IPass

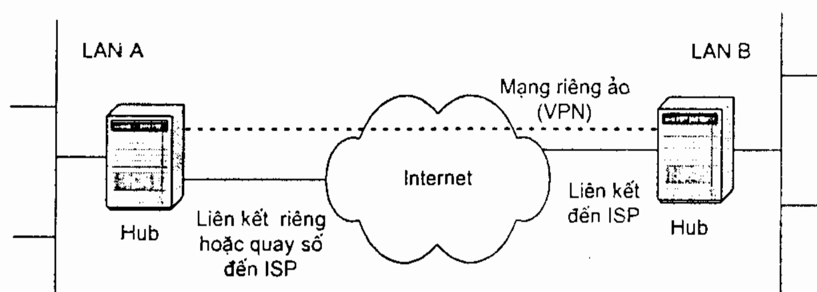
2.2 Nối các mạng trên Internet (Intranet VPN)

Có hai phương pháp sử dụng mạng VPN để kết nối các mạng cục bộ LAN (Local Area Network) tại các điểm cuối ở xa.

- Dùng các đường kênh thuê riêng để nối một văn phòng chi nhánh đến mạng LAN công ty: các văn phòng chi nhánh và các bộ định tuyến có thể sử dụng một mạch dành riêng cục bộ và ISP địa phương để kết nối đến Internet. Phần mềm VPN sử dụng các cuộc nối ISP nội bộ và Internet công cộng để tạo một VPN giữa các văn phòng chi nhánh và bộ định tuyến của các hub hợp nhất.

- Dùng đường dây quay số để kết nối một văn phòng chi nhánh đến một LAN: bộ định tuyến ở văn phòng chi nhánh quay số đến ISP, phần mềm VPN sử dụng cuộc nối đến ISP để tạo một VPN giữa bộ định tuyến của văn phòng chi nhánh và bộ định tuyến của hub thông qua Internet.

Chú ý: Trong cả hai trường hợp, cơ sở hạ tầng để nối văn phòng chi nhánh và các văn phòng liên kết đến Internet mang tính cục bộ. Cả VPN dạng client-server (máy trạm - máy chủ) và server-server (máy chủ - máy chủ) sẽ tiết kiệm được chi phí rất lớn trong việc sử dụng phương thức truy cập quay số. Các máy chủ VPN được nối đến ISP bằng một đường kênh thuê riêng (leased line) và phải hoạt động 24/24 để nhận luồng dữ liệu đến.



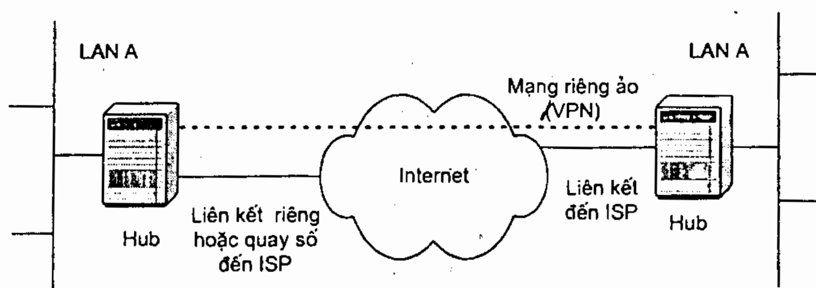
Hình 2.4: Dùng VPN để kết nối 2 vị trí từ xa

2.3 Nối các máy tính trên một Intranet (Extranet VPN)

Trong một số các liên kết mạng, một số các người dùng trong LAN của một phòng, ban nào đó không được kết nối bằng đường truyền vật lý thì sẽ nảy sinh vấn đề về khả năng truy cập thông tin của người dùng đó.

VPN sẽ cho phép các LAN được kết nối vật lý đến mạng hợp nhất và được phân chia bởi một máy chủ VPN. Chú ý rằng, máy chủ VPN không hoạt động giống như một bộ định tuyến giữa các mạng hợp nhất và các LAN. Một bộ định tuyến sẽ kết nối đến hai mạng, cho phép quyền truy cập đến LAN. Bằng cách sử dụng một VPN, người quản trị mạng có thể đảm bảo rằng chỉ có những người dùng đó trên các mạng hợp nhất có các tiêu chuẩn phù hợp (dựa trên một chính sách của công ty) có thể thiết lập một VPN với máy chủ VPN và truy cập được

đến các tài nguyên được bảo vệ của phòng ban đó. Thêm vào đó, tất cả dữ liệu trong VPN được đóng góp một cách tin cậy. Những người dùng nào không có các quyền thích hợp không thể xem được LAN.



Hình 2.5: Dùng VPN để kết nối 2 máy tính từ xa trong cùng một LAN

Tất cả hoạt động kinh doanh hoạt động ở cơ chế giống như trong một mạng riêng, bao gồm các vấn đề về bảo mật, chất lượng dịch vụ QoS (Quality of Sevice), quản trị và độ tin cậy.

CHƯƠNG 3

KIẾN TRÚC CỦA MỘT MẠNG RIÊNG ẢO VPN

Hai thành phần cơ bản của Internet tạo nên các mạng riêng ảo VPN, đó là:

- Thứ nhất, là tiến trình được biết đến như định đường hầm (tunneling) cho phép làm "ảo" một VPN.
- Thứ hai, đó là những dịch vụ bảo mật đa dạng nhằm giữ cho dữ liệu của VPN được bảo mật - riêng (private).

3.1 Kiến trúc của một mạng VPN

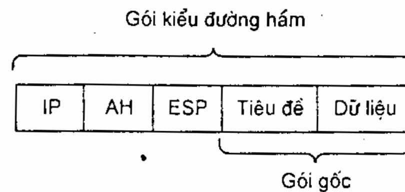
3.1.1 Đường hầm: phần ảo trong VPN

Trong mạng riêng ảo VPN, "ảo" - virtual mang ý nghĩa là mạng linh động, với các kết nối được thiết lập dựa trên nhu cầu tổ chức. Không như những kết nối sử dụng đường kênh thuê riêng trong các mạng VPN truyền thống, Internet VPN không duy trì những kết nối thường trực giữa các điểm cuối tạo thành mạng công ty (corporate network). Thay vào đó, một kết nối được tạo ra giữa hai site khi cần đến. Và khi kết nối này không còn cần thiết nữa thì nó sẽ bị hủy bỏ, làm cho băng thông và các tài nguyên mạng khác sẵn sàng cho những kết nối khác sử dụng.

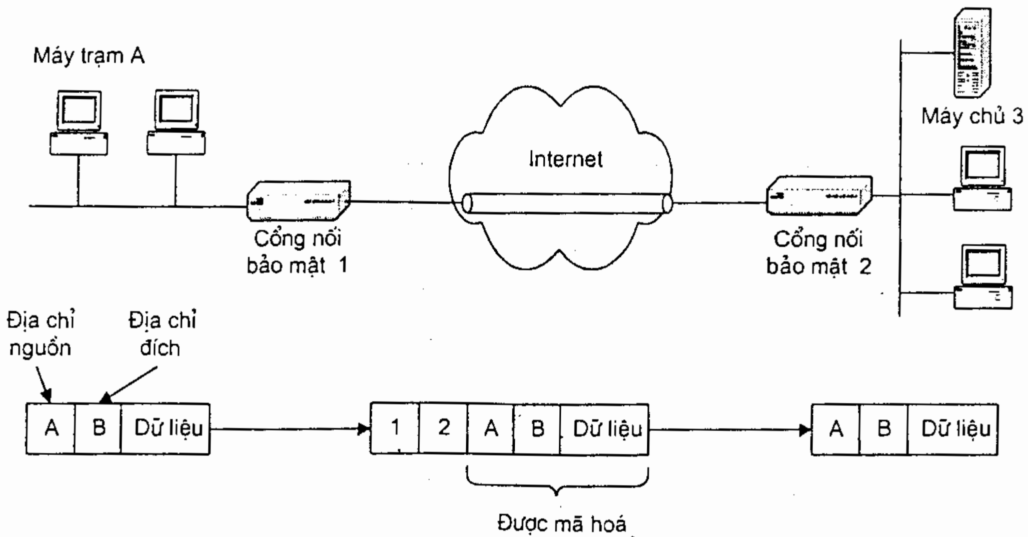
Ảo - "virtual" cũng mang ý nghĩa rằng cấu trúc logic của mạng được hình thành chỉ cho những thiết bị mạng tương ứng của mạng đó, bất chấp cấu trúc vật lý của mạng cơ sở (trong trường hợp này là Internet). Các thiết bị như bộ định tuyến (router), chuyển mạch (switch) hay những thành phần mạng của các ISP được giấu đi khỏi những thiết bị và người dùng của mạng ảo. Do đó, những kết nối tạo nên mạng riêng ảo VPN không có cùng tính chất vật lý với những kết nối cố định (hard-wired) được dùng trong mạng LAN. Việc che giấu cơ sở hạ tầng của ISP và Internet được thực hiện bởi một khái niệm gọi là định đường hầm (tunneling).

Những đường hầm được sử dụng cho các dịch vụ khác trên Internet bên cạnh VPN, như quảng bá IP (IP multicasting) và IP di động (mobile IP). Việc tạo đường hầm tạo ra một kết nối đặc biệt giữa hai điểm cuối. Để tạo ra một đường hầm, điểm cuối nguồn phải đóng gói (encapsulate) các gói (packet) của mình trong những gói IP (IP packet) cho việc truyền qua Internet. Đối với mạng riêng ảo - VPN, việc đóng gói (encapsulation) có thể bao gồm việc mã hoá gói gốc (original) và thêm vào một tiêu đề IP (IP header) mới cho gói (hình 3.1). Tại điểm cuối nhận, cổng nối (gateway) gỡ bỏ tiêu đề IP và giải mã gói nếu như cần thiết và chuyển gói nguyên thủy đến đích của nó (hình 3.2).

Việc tạo đường hầm cho phép những dòng dữ liệu và những thông tin người dùng kết hợp được truyền trên một mạng chia sẻ trong một ống ảo (virtual pipe). Ống này làm cho việc định tuyến trên mạng hoàn toàn trở nên trong suốt đối với người dùng.



Hình 3.1: Định dạng gói cho việc tạo đường hầm



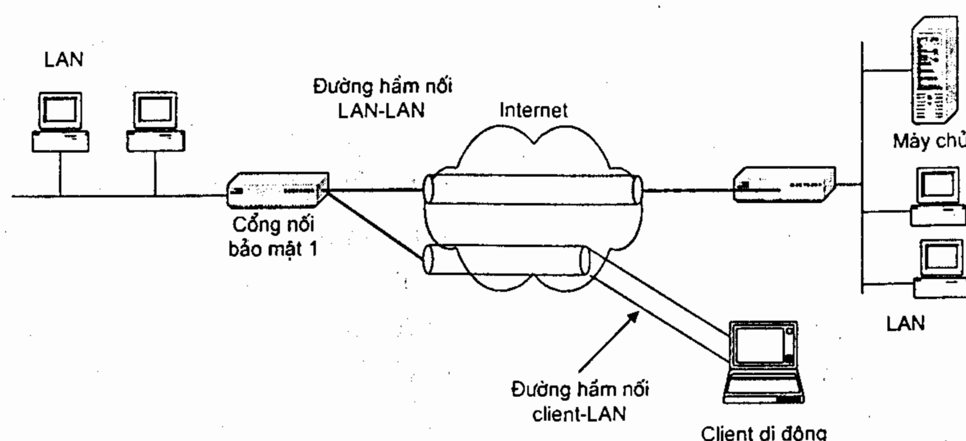
Hình 3.2: Cấu trúc một đường hầm

Thông thường, những đường hầm được định nghĩa là một trong hai loại sau: thường trực (permanent), tạm thời (temporary). Những đường hầm tĩnh (static tunnel) thuộc loại thường trực ít được sử dụng trong VPN, bởi vì chúng sẽ chiếm

dụng băng thông ngay cả khi không được sử dụng. Đường hầm tạm thời hay còn gọi là đường hầm động (dynamic tunnel) được quan tâm và hữu dụng hơn cho VPN, bởi vì loại đường hầm này có thể được thiết lập khi cần đến và sau đó được hủy bỏ khi không còn nhu cầu, ví dụ như khi một phiên thông tin được kết thúc. Vì thế, những đường hầm động không yêu cầu đặt trước băng thông cố định. Bởi vì nhiều ISP cung cấp những kết nối có giá phụ thuộc vào băng thông trung bình sử dụng trên một kết nối, đường hầm động có thể giảm băng thông sử dụng và dẫn đến giá thấp hơn.

Những đường hầm có thể bao gồm hai kiểu điểm cuối, có thể là một máy tính cá nhân hay một mạng LAN với một cổng nối bảo mật mà cổng nối này có thể là một bộ định tuyến hay tường lửa. Tuy nhiên chỉ có hai kiểu kết hợp của những điểm cuối này thường được xem xét trong thiết kế VPN. Trong trường hợp đầu tiên, đường hầm kết nối LAN-LAN, một cổng nối bảo mật tại mỗi điểm cuối phục vụ như bộ giao tiếp giữa đường hầm với mạng LAN riêng (hình 3.3). Trong những trường hợp như vậy, người dùng trên các LAN có thể dùng đường hầm một cách trong suốt để thông tin với nhau.

Trong trường hợp thứ hai, đó là những đường hầm kết nối client-LAN, đây là kiểu thường thiết lập cho người dùng di động (mobile user) muốn kết nối với mạng LAN công ty (corporate LAN). Client khởi tạo việc tạo đường hầm trên đầu cuối của mình để trao đổi lưu lượng với mạng công ty. Để làm được việc này, người dùng phải chạy một chương trình client đặc biệt trên máy tính của người dùng để thông tin với cổng nối bảo mật để đến mạng LAN đích.



Hình 3.3: LAN và client: các đường hầm VPN

3.1.2 Các dịch vụ bảo mật: tính riêng trong VPN

Quan trọng ngang với việc sử dụng một mạng riêng ảo - VPN, thậm chí không muốn nói là quan trọng hơn, là việc đưa ra tính riêng tư hay bảo mật.

Trong hầu hết các sử dụng cơ bản của nó, tính "riêng tư" trong VPN mang ý nghĩa là một đường hầm giữa 2 người dùng trên một mạng VPN xuất hiện như một liên kết riêng (private link), thậm chí nó có thể chạy trên môi trường dùng chung (shared media). Nhưng đối với việc sử dụng của các nhà kinh doanh, đặc biệt cho kết nối LAN-LAN, "riêng" phải mang ý nghĩa hơn điều đó, nó phải có nghĩa là bảo mật, đó là thoát khỏi những con mắt tò mò và can thiệp.

Mạng VPN cần cung cấp bốn chức năng giới hạn để đảm bảo độ bảo mật cho dữ liệu. Bốn chức năng đó là:

- Xác thực (Authentication): đảm bảo dữ liệu đến từ một nguồn yêu cầu.
- Điều khiển truy cập (Access control): hạn chế việc đạt được quyền cho phép vào mạng của những người dùng bất hợp pháp.
- Tin cậy (Confidentiality): ngăn không cho một ai đó đọc hay sao chép dữ liệu khi dữ liệu được truyền đi qua mạng Internet.
- Tính toàn vẹn của dữ liệu (Data integrity): đảm bảo không một ai làm thay đổi dữ liệu khi nó truyền đi trên mạng Internet.

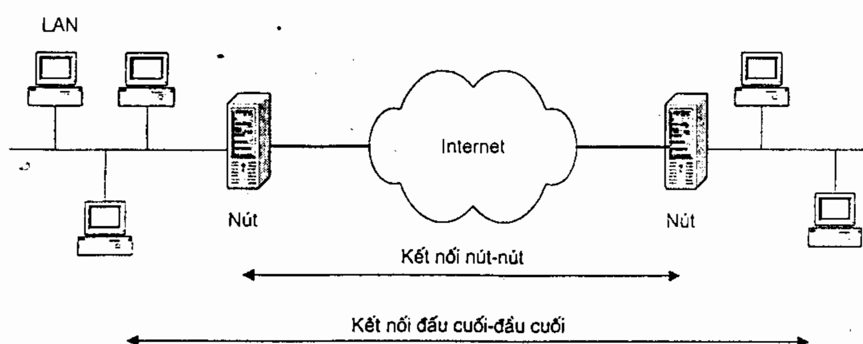
Mặc dù những đường hầm có thể làm cho việc truyền dẫn dữ liệu qua mạng Internet bảo mật, nhưng việc xác thực người dùng và duy trì tính toàn vẹn dữ liệu phụ thuộc vào các tiến trình mật mã (cryptographic), ví dụ như chữ ký điện tử và mật mã (encryption). Những tiến trình này sử dụng những điều bí mật được chia sẻ gọi là các khoá (key), các khoá này phải được quản lý và phân phối cẩn thận, hơn nữa được thêm vào việc quản lý các nhiệm vụ của một mạng VPN.

Các dịch vụ bảo mật một mạng Internet VPN gồm: xác thực (authentication), mã hoá (encryption) và toàn vẹn dữ liệu (data integrity) được cung cấp tại lớp 2 - lớp liên kết dữ liệu (Data-link) và lớp 3 - lớp mạng (Network) của mô hình OSI. Việc phát triển các dịch vụ bảo mật tại các lớp thấp của mô hình OSI làm cho các dịch vụ này trở nên trong suốt hơn đối với người dùng.

Nhưng việc thực hiện bảo mật tại những mức độ này có thể diễn ra hai hình thức mà nó tác động đến trách nhiệm của một cá nhân cho việc bảo mật dữ liệu của riêng mình. Bảo mật có thể được thực hiện cho các thông tin đầu cuối-đến-đầu cuối (end-to-end communication), ví dụ như giữa hai máy tính, hay giữa các thành phần mạng khác với nhau, ví dụ như tường lửa hay bộ định tuyến. Trong trường hợp cuối có thể được xem như bảo mật kết nối nút-nút (node-to-node security) trong hình 3.4.

Việc dùng các biện pháp bảo mật trên cơ sở kết nối nút-nút có thể làm cho những dịch vụ bảo mật trong suốt hơn đối với người dùng cuối và làm nhẹ bớt những yêu cầu làm nặng tải, ví dụ như mã hoá (encryption). Nhưng việc bảo mật kết nối nút-nút yêu cầu những mạng đằng sau nút phải là những mạng có độ tin cậy. Việc

bảo mật đầu cuối-đầu cuối thì vốn đã bảo mật hơn kết nối nút-nút, vì nó bao gồm mỗi máy trạm, người gửi và người nhận một cách trực tiếp. Tuy nhiên việc bảo mật kết nối client-client có những điểm bất lợi, đó là nó làm tăng sự phức tạp của người dùng cuối và nó có thể gây khó khăn hơn cho việc quản lý.



Hình 3.4: So sánh bảo mật nút-nút và đầu cuối-đầu cuối

3.2 Các giao thức của một mạng Internet VPN

3.2.1 Các giao thức đường hầm và bảo mật

Bốn giao thức được đề nghị lúc ban đầu như những giải pháp cho mạng VPN. Trong đó ba giao thức được thiết kế để làm việc ở lớp thứ 2, lớp liên kết dữ liệu, gồm: giao thức chuyển tiếp lớp 2 - L2F (Layer 2 Forwarding), giao thức định đường hầm điểm-điểm PPTP (Point-to-Point Tunneling Protocol) và giao thức định đường hầm lớp 2 L2TP (Layer 2 Tunneling Protocol). Giao thức mạng VPN duy nhất cho lớp 3 là IPSec, được phát triển bởi IETF vài năm trước đây. Tất cả các giao thức được trình bày trong bảng 3.1.

Trong đó những chi tiết của những giao thức này được xem xét một cách kỹ lưỡng trong những chương sau, sau đây là một số đặc điểm của các giao thức này

- PPTP là một cơ chế xây dựng đường hầm điểm-điểm được tạo ra trước tiên để hỗ trợ các gói đường hầm (packet tunneling) trong phần cứng máy chủ truy cập từ xa của hãng Ascend và phần mềm Microsoft Windows NT.
- Giao thức định đường hầm lớp 2 lai ghép (Hybrid Layer 2 tunneling) còn gọi là giao thức định đường hầm lớp 2 (Layer 2 Tunneling Protocol) được Cisco phát triển từ giao thức L2F của họ.
- IPSec là một tiêu chuẩn được tạo ra để thêm vào tính bảo mật cho mạng TCP/IP.

Bảng 3.1: So sánh các giao thức VPN

Tên	Điểm mạnh	Điểm yếu	Sử dụng trong mạng
IPSec	+ Chuẩn giao thức rãnh. + Hoạt động một cách độc lập của các ứng dụng mức cao hơn. + Cho phép giấu địa chỉ mạng mà không cần sử dụng dịch địa chỉ mạng (NAT) + Sẽ đáp ứng phát triển các kỹ thuật mã hoá.	+ Không có quản lý người dùng. + Ít sản phẩm có khả năng tương tác giữa các nhà cung cấp. + Ít hỗ trợ giao diện (desktop support).	+ Phần mềm tốt nhất trên máy tính người dùng cho các giải pháp độc quyền của nhà cung cấp đối với việc truy cập từ xa bằng quay số (dial-up).
PPTP	+ Chạy trên nền Windows NT, Windows 95 và Windows 98. + Cung cấp cho đầu cuối-đến-đầu cuối và định đường hầm kết nối nút-nút. + Các đặc điểm giá trị được thêm vào phổ biến cho truy cập từ xa. + Sử dụng những miền người dùng Windows có sẵn cho việc xác thực. + Cung cấp khả năng đa giao thức (multiprotocol capability). + Sử dụng mã hoá RSA RC-4.	+ Không cung cấp mã hoá dữ liệu từ những máy chủ truy cập từ xa. + Mang tính độc quyền rộng lớn, yêu cầu một máy chủ chạy Win NT để kết thúc những đường hầm. + Chỉ sử dụng mã hoá bằng RSA RC-4.	+ Được dùng tại các máy chủ truy cập từ xa cho định đường hầm proxy. + Có thể được dùng giữa các văn phòng ở xa mà có sử dụng các máy chủ Win NT để chạy máy chủ truy cập từ xa và định tuyến RRAS (Routing and Remote Access Server). + Có thể dùng cho những máy để bàn Win9x hay máy trạm dùng Win NT.
L2F	+ Cho phép định đường hầm đa giao thức + Được cung cấp bởi nhiều nhà cung cấp.	+ Không có mã hoá. + Yếu trong việc xác thực người dùng (user authentication). + Không có điều khiển luồng cho đường hầm (tunnel flow control)	+ Dùng cho truy cập từ xa tại POP.
L2TP	+ Kết hợp PPTP và L2F. + Chỉ cần một gói dựa trên mạng để chạy trên X25 và Frame relay. + Sử dụng IPSec cho việc mã hoá (encryption).	+ Chưa được cung cấp trong nhiều sản phẩm. + Không bảo mật ở những đoạn cuối.	+ Dùng cho truy cập từ xa tại POP.

3.2.2 Các giao thức quản trị

Việc duy trì quyền truy cập của người dùng trong mạng và thông tin bảo mật liên quan đến họ, ví dụ như các khoá mật mã (cryptographic key) là một vấn đề quản lý quyết định trong các mạng VPN. Hai họ giao thức khác nhau hiện nay được sử dụng tùy theo loại mạng VPN đang được quản lý. Đối với mạng quay số VPN hay kết nối client-LAN dùng đường hầm PPTP và L2TP, có một giao thức gọi là RADIUS có thể được dùng cho việc xác thực (authentication) và tính cước (accounting). Đối với mạng VPN kết nối LAN-LAN, giao thức ISAKMP/Oakley được sử dụng là một biến thể của IPSec.

Công cụ phổ biến nhất cho việc xác thực và tính cước đối với việc truy cập từ xa là xác thực dịch vụ người dùng quay số từ xa RADIUS (Remote Authentication Dial-In User Service) và đây là giao thức thích hợp cho người dùng sử dụng đường hầm quay số, như PPTP và L2F.

RADIUS hỗ trợ việc xác thực và tính cước bằng một cơ sở dữ liệu lưu trữ các tệp cấu hình (profile) truy cập của tất cả người dùng tin cậy. Thông tin trên mỗi tệp cấu hình của người dùng bao gồm mật khẩu (password), quyền truy cập (access privilege), cho phép và cách sử dụng mạng (network usage) cho việc tính cước. Thiết bị truy cập mạng tương tác với máy chủ RADIUS một cách bảo mật, trong suốt và tự động. Khi một người dùng có ý định đăng nhập vào mạng từ xa, chuyển mạch truy cập mạng (network access switch) truy vấn máy chủ RADIUS để thu thập tệp cấu hình của người dùng cho việc xác thực và cấp quyền. Một RADIUS proxy để cho máy chủ RADIUS tại một nhà cung cấp dịch vụ truy cập một máy chủ RADIUS của một cơ quan để thu thập bất kỳ thông tin cần thiết của người dùng, những thông tin này cần thiết cho việc bảo mật mạng VPN dựa trên Internet.

Như đã đề cập trước đây, nhiều phương pháp xác thực và mã hoá sử dụng trong mạng VPN yêu cầu xác định và phân phối của các khoá. Đối với những hệ thống nhỏ, việc phân phối các khoá được thực hiện bằng tay, trên một cuộc thoại bảo mật, hay qua một người thông tin cũng đáp ứng được, nhưng đối với những mạng VPN lớn thì các hệ thống tự động cần thiết hơn. Mặc dù không có một tiêu chuẩn nào được yêu cầu cho việc quản lý khoá nhân công (manual key), nhưng vài chuẩn hoá được yêu cầu cho những hệ thống tự động, một phần bởi vì tất cả các thiết bị truy cập mạng hầu hết tương tác một cách thường xuyên và tự động với hệ thống quản lý khoá (key-management system).

3.3 Các khối trong mạng VPN

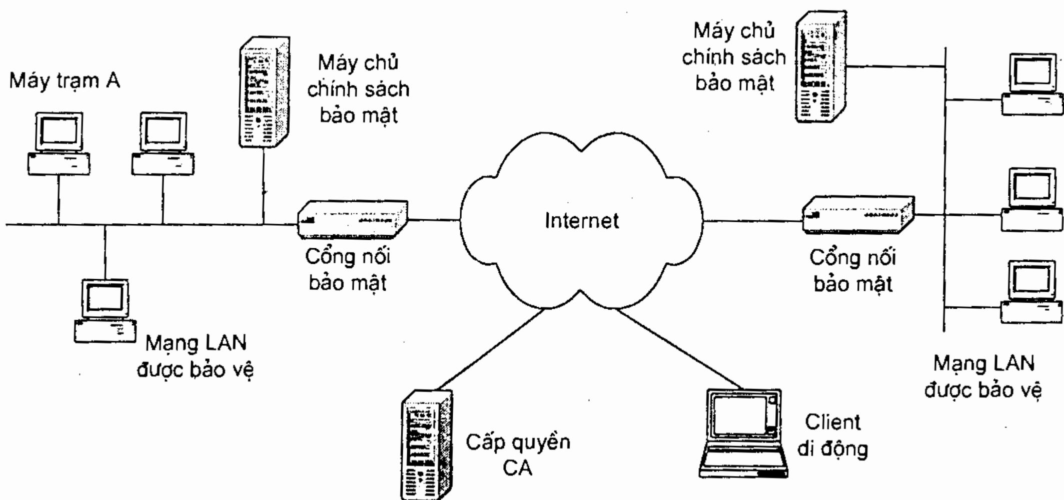
Theo hình 3.5, chúng ta thấy có bốn thành phần chính của một mạng Internet VPN, đó là: Internet, cổng nối bảo mật (security gateway), máy chủ

chính sách bảo mật (security policy server) và cấp quyền CA (certificate authority).

3.3.1 Internet

Có nhiều kiểu của nhà cung cấp dịch vụ Internet (ISP) khác nhau, được xếp loại từ các ISP nội hạt nhỏ đến các ISP vùng và ISP quốc gia hay trên quốc gia, tất cả được sắp xếp thành những bậc (tier) tuỳ thuộc vào khả năng của các ISP này.

Nhà cung cấp bậc một, ví dụ như FiberNet, AT&T, IBM, GTE Internetworking, ISP sở hữu và vận hành các mạng quốc gia riêng cùng với việc mở rộng các mạng xương sống quốc gia. Những mạng độc lập này gặp nhau và liên mạng với nhau tại điểm truy cập mạng của Internet NAP (Network Access Point). Qua những thỏa thuận ngang hàng giữa các công ty riêng này, trao đổi có thứ tự các luồng tín hiệu số được trở nên dễ dàng giữa các mạng khác nhau.

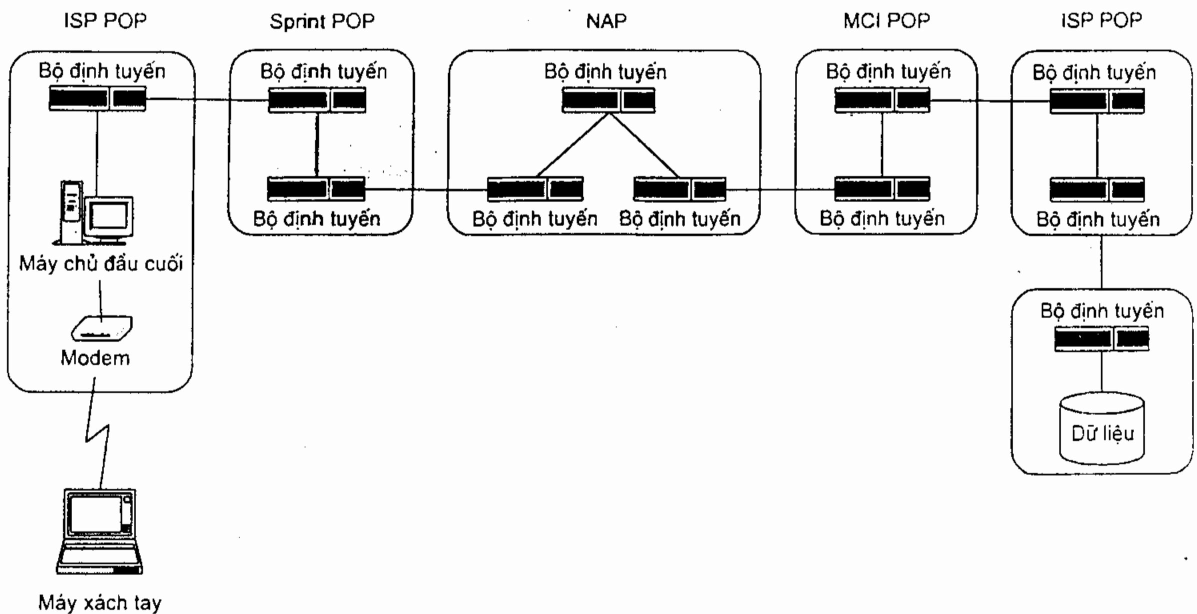


Hình 3.5: Các thành phần trong một mạng Internet VPN

Nhà cung cấp bậc hai là một công ty mua kết nối Internet từ một trong những nhà cung cấp bậc 1, cung cấp truy cập quay số ở nhà riêng (residential dial-up access) hay đưa lên các trang Web hoặc bán lại băng thông. Điều lưu ý quan trọng là không có điểm Internet NAP nào cung cấp liên kết Internet cho người dùng bình thường hay cho nhà kinh doanh và công nghiệp. Những điểm NAP chỉ là những điểm dùng cho việc trao đổi lưu thoại một cách thứ tự giữa những tổ chức duy trì toàn mạng đường trục quốc gia. Điểm NAP không là điểm mà tại đó các nhà kinh doanh hay những cá nhân có thể thu lợi từ việc truy cập Internet. Ngoài ra, những kết nối đến các điểm Internet NAP được thực hiện tại tốc độ thấp nhất của DS-3 (45 Mbit/s). Mục đích của những điểm Internet NAP là

làm cho việc trao đổi lưu lượng giữa mạng này đến mạng khác trở nên dễ dàng, chứ không phải để bán liên kết Internet.

Để trở thành một điểm NAP công nghiệp (industry-recognized NAP) yêu cầu đầu tư lớn vào thiết bị chuyển mạch lớp 2 (Layer 2 switching equipment) và những phương tiện POP. Điển hình là, những phương tiện này có những đường cáp quang đa sóng mang dự phòng (multiple carrier), hỗ trợ kết nối kích thước tăng (circuit sized up) và bao gồm OC-48 (2.4 Gbit/s).

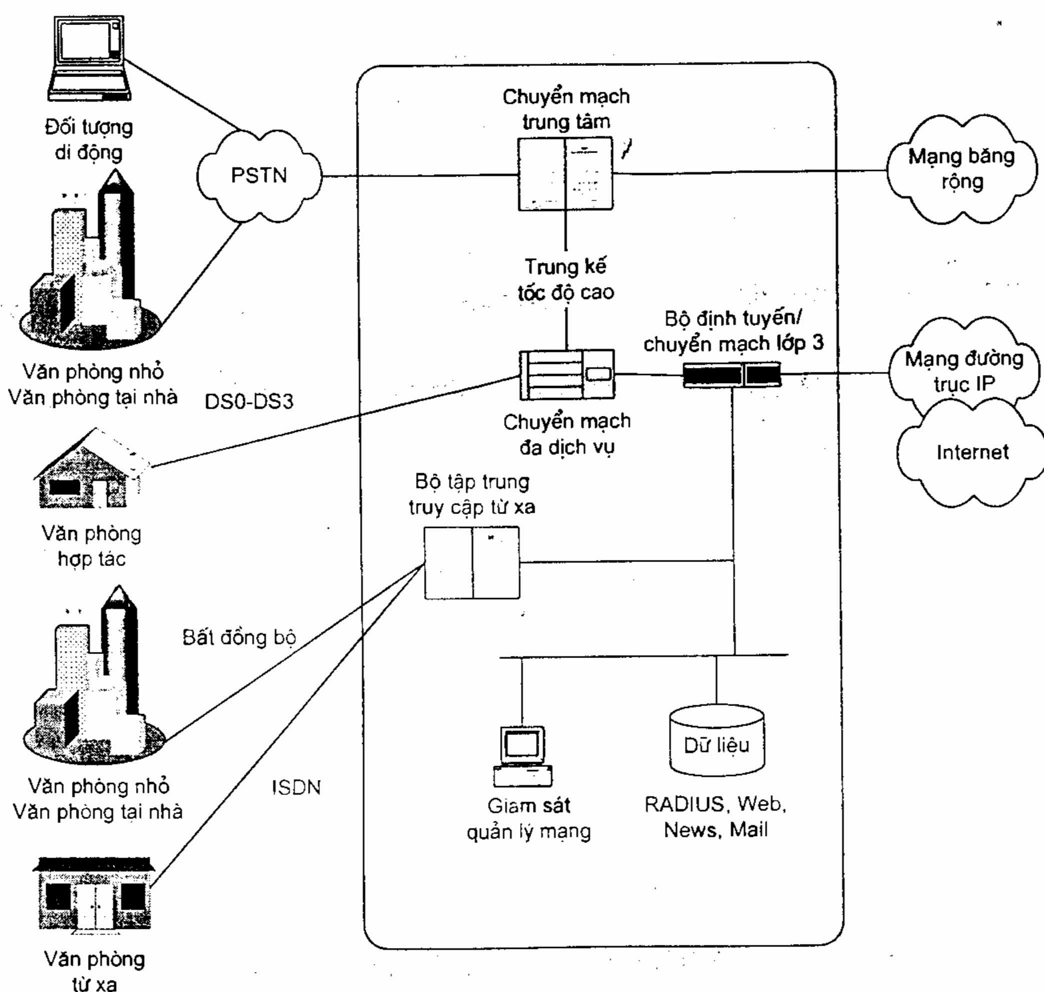


Hình 3.6: Truyền thông qua các ISP, POP và NAP

Hình 3.6 mô tả việc dữ liệu được truyền từ một người dùng sử dụng modem quay số đến điểm kết nối POP của một ISP để kết nối vào Internet và vào mạng VPN. Dữ liệu được chuyển từ máy xách tay (laptop) của người dùng đến điểm POP cục bộ và sau đó đến mạng Internet vùng (regional Internet network) và có thể qua một vài điểm POP khác để điểm NAP thích hợp trước khi nó được định tuyến điểm POP khác gần với đích chỉ định hơn. Có hai lý do đáng kể cho tất cả tiến trình trên: trước tiên, những ISP khác nhau quản lý những mạng tạo nên Internet hợp tác với nhau; thứ hai, những đặc điểm địa chỉ được tìm thấy trong giao thức IP thích hợp, giúp nối kết các mạng lại với nhau.

Cho dù người dùng là một cá nhân làm việc tại nhà hay trên đường quay số vào Internet hay là nhà kinh doanh với kết nối suốt ngày đến Internet. Tại điểm POP, ISP điều khiển các kiểu khác nhau của môi trường mà khách hàng sử dụng cho việc truy cập Internet và gửi chuyển tiếp lưu lượng của khách hàng đến mạng

đường trục đã được kết nối với phần còn lại của mạng Internet tại một vài điểm (hình 3.7).



Hình 3.7: Cấu trúc của một ISP POP thông dụng

Điểm POP gồm có những thiết bị khác nhau cho mỗi môi trường truyền dẫn nó hỗ trợ, ví dụ như một dải modem cho các phiên quay số và CSU/DSU cho Frame Relay và DDS; những ISP khác chọn lựa không hỗ trợ cho môi trường khác biệt đến mạng công cộng, thay vào đó quản lý một đường kênh thuê riêng đến những điểm POP của họ. Để quản lý những môi trường khác nhau cho lưu lượng người dùng, POP bao gồm các bộ định tuyến, các chuyển mạch IP để kết nối mạng LAN cục bộ của POP đến phần còn lại của mạng của ISP như điều khiển quản lý mạng (network management console). Trong một số trường hợp, POP bao gồm những máy chủ cho việc đang tải các trang Web, thư điện tử, tin tức, ... và những máy chủ xác thực RADIUS cho khách hàng của ISP.

3.3.2 Các cổng nối bảo mật

Các cổng nối bảo mật (security gateway) được đặt giữa các mạng công cộng và mạng riêng, ngăn chặn xâm nhập trái phép vào mạng riêng. Chúng cũng có thể cung cấp những khả năng tạo đường hầm và mã hoá dữ liệu riêng (private data) trước khi được chuyển đến mạng công cộng.

Nói chung, một cổng nối bảo mật cho mạng VPN gồm một trong những loại sau: bộ định tuyến, tường lửa, phần mềm tích hợp VPN và phần mềm VPN.

Vì những bộ định tuyến phải kiểm tra và xử lý mỗi gói rời khỏi LAN, gồm quá trình mã hoá gói (packet encryption) trên bộ định tuyến. Những nhà cung cấp của các dịch vụ VPN dựa trên bộ định tuyến thường đưa ra hai loại sản phẩm: phần mềm thêm vào hay một mạch điện thêm vào với một phương tiện mã hoá trên cơ sở đồng xử lý (coprocessor-based encryption engine). Sản phẩm sau thích hợp nhất cho những vị trí yêu cầu năng suất truyền lớn hơn.

Nhiều nhà cung cấp tường lửa có một đường hầm mạnh trong sản phẩm của họ. Giống như bộ định tuyến, các tường lửa phải xử lý tất cả luồng IP để truyền luồng dữ liệu dựa trên các bộ lọc được định nghĩa cho tường lửa. Bởi vì tất cả tiến trình được thực hiện bởi tường lửa, không thích hợp cho việc xây dựng đường hầm trên những mạng lớn có một lưu lượng lớn. Việc kết hợp tạo đường hầm và mã hoá (encryption) với tường lửa có lẽ chỉ được sử dụng tốt nhất cho các mạng nhỏ với lưu lượng thấp.

Giải pháp VPN khả thi khác là sử dụng phần cứng đặc biệt được thiết kế cho nhiệm vụ tạo đường hầm và mã hoá (encryption). Những thiết bị thường hoạt động như những cầu mã hoá được đặt giữa các bộ định tuyến mạng với các kết nối WAN. Mặc dù hầu hết các thiết bị phần cứng này được thiết kế cho các cấu hình kết nối LAN-LAN, nhưng vài sản phẩm cũng hỗ trợ cho việc tạo đường hầm của kết nối client-LAN.

Cuối cùng, những hệ thống phần mềm VPN thường là những chọn lựa giá thấp trong những môi trường tương đối nhỏ và không phải xử lý nhiều lưu lượng. Những giải pháp này có thể hoạt động trên những máy chủ có sẵn và chia sẻ các tài nguyên với nhau và được xem là khởi đầu tốt cho mạng VPN.

3.3.3 Các thành phần bảo mật khác

Thành phần quan trọng khác của một mạng VPN là máy chủ chính sách bảo mật (security policy server). Máy chủ này bảo quản các danh sách điều khiển truy cập và thông tin khác liên quan đến người dùng mà cổng nối dùng để xác định lưu lượng nào được cho phép. Đối với một số hệ thống, ví dụ như những hệ

thống dùng PPTP, việc truy cập có thể được điều khiển thông qua một máy chủ RADIUS, khi IPSec được sử dụng, máy chủ có trách nhiệm đối với việc quản lý các khoá dùng chung cho mỗi phiên làm việc.

Các công ty có thể chọn lựa để bảo quản cơ sở dữ liệu các chứng nhận điện tử của riêng họ cho người dùng bằng cách cài đặt một máy chủ chứng nhận công ty (corporate certificate server). Đối với những nhóm người dùng nhỏ, việc xác thực của các khoá dùng chung có thể yêu cầu việc kiểm tra với một thành viên thứ ba đang duy trì những chứng nhận điện tử được kết hợp với các khoá được mật mã dùng chung; những thành viên thứ ba này được gọi là những "giấy chứng nhận" CA (certificate authorities). Nếu một mạng VPN của công ty phát triển trong một mạng Extranet, thì một "giấy chứng nhận" bên ngoài có thể được dùng để xác thực những người dùng từ những hội viên kinh doanh của công ty đó.

3.4 Minh họa kiến trúc truy cập VPN theo đề nghị của Cisco

3.4.1 Xây dựng các khối trong truy cập VPN

Các khối này làm nền cho các ứng dụng thương mại, nó yêu cầu khả năng tuân theo các quy định giống nhau như một mạng riêng.

3.4.2 Bảo mật

Vấn đề quan trọng nhất trong truy cập VPN là đảm bảo độ bảo mật trên đường truyền từ đầu cuối của thuê bao. Nếu một mạng cung cấp một mức bảo mật giới hạn ở các lớp cao thì nhà cung cấp sẽ không thể đảm bảo tính toàn vẹn của một dịch vụ truy cập VPN.

3.4.2.1 Kiến trúc xác thực

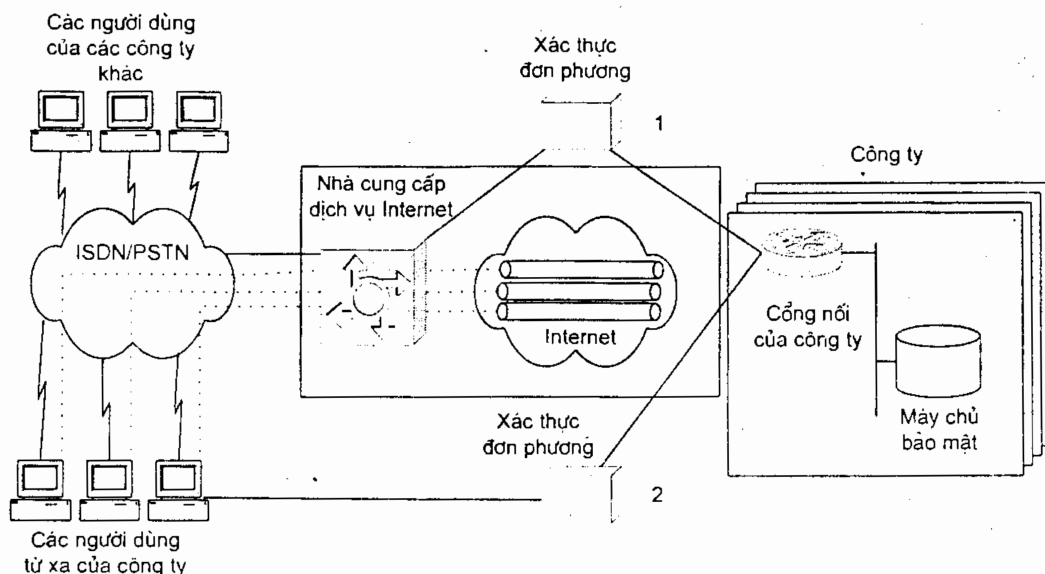
Trong một môi trường truy cập VPN, khía cạnh bảo mật quan trọng nhất liên quan đến việc nhận dạng ra một người dùng như một thành viên của một công ty và thiết lập một đường hầm đến cổng nối của công ty. Cổng nối này phải có khả năng xác thực các người dùng, các quyền truy cập và tính cước (AAA).

Xác thực đơn phương

Xác thực người dùng là một điểm quan trọng của truy cập VPN. Để xác định xác thực này, đầu tiên client sẽ thiết lập một kết nối đến mạng cung cấp dịch vụ thông qua một POP, sau đó thiết lập một kết nối thứ hai với mạng khách hàng.

Các điểm cuối đường hầm trong truy cập VPN xác thực với nhau. Kế tiếp, các người dùng kết nối đến các thiết bị đầu cuối khách hàng (CPE). Các cổng nối người dùng sử dụng giao thức phân tích chất lượng thành viên hay giao thức Internet tuyến nối tiếp SLIP (Serial Line Internet Protocol) và được xác thực

thông qua một giao thức xác định tên/mật khẩu như PAP (Password Authentication Protocol), giao thức xác thực yêu cầu bắt tay CHAP (Challenge Handshake Authentication Protocol) hay hệ thống điều khiển truy cập bộ điều khiển truy cập đầu cuối TACACS+ (Terminal Access Controller Access Control System Plus). Các cổng nối công ty duy trì một giao tiếp với máy chủ điều khiển từ xa (ACS), máy chủ AAA, sử dụng giao thức TACACS hay RADIUS.



Hình 3.8: Xác thực đơn phương

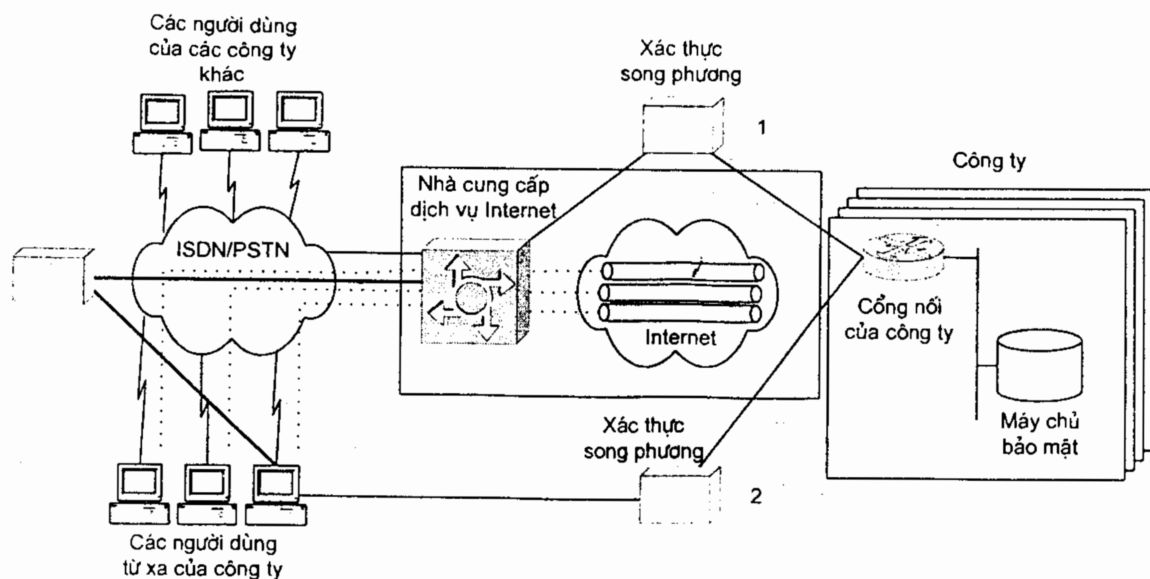
Tại các điểm này, các quyền được thiếp lập sử dụng cơ chế được lưu trữ trong ACS và liên lạc đến cổng nối ở đầu cuối khách hàng. Thường thì các khách hàng quản trị máy chủ ACS cung cấp những yêu cầu cơ bản và điều kiện nào có thể truy cập mạng cũng như những máy chủ nào được truy cập.

Các tập tin cấu hình (profile) người dùng xác định người dùng nào có thể được làm việc trên mạng. Người dùng được cấp quyền, mạng tạo ra một giao tiếp ảo cho mỗi người dùng.

Xác thực song phương

Trong một số trường hợp, việc xác thực song phương sử dụng thích hợp hơn trong việc xác thực (hình 3.9).

Đầu tiên, người dùng sẽ quay số đến điểm truy cập POP của ISP, sau đó ISP sẽ nhận diện người gọi thông qua một số nhận diện chung. Máy chủ truy cập mạng NAS (Network Access Server) sẽ biết được số nhận diện này thuộc mạng khách hàng nào. Kế tiếp, NAS sẽ thiết lập một đường hầm với cổng nối phía khách hàng. Cuối cùng, người dùng được xác thực lần thứ hai bởi cổng nối phía mạng của công ty.



Hình 3.9: Xác thực song phương

3.4.2.2 Các sản phẩm bảo mật và các kỹ thuật cho truy cập VPN

Tường lửa

Cisco IPX Firewall - sử dụng một hệ thống không-Unix, bảo mật và thời gian thực, cho phép 64,000 kết nối hoạt động cùng một lúc. Ưu điểm của các dòng sản phẩm Cisco PIX firewall là một cơ chế bảo mật dựa trên thuật toán bảo mật tương thích ASA (Adaptive Security Algorithm), thuật toán này bảo mật một cách hiệu quả truy cập đến các máy mạng nội bộ.

Cisco IOS Firewall Feature Set - cung cấp một giải pháp tích hợp cho các nhà cung cấp dịch vụ nhỏ và cho các chi nhánh văn phòng môi trường cỡ nhỏ và các văn phòng trang bị thiết bị đầu cuối khách hàng (CPE) ở xa. Cisco IOS Firewall Feature Set làm nổi bật các dịch vụ bảo mật của Cisco IOS, cung cấp hỗ trợ các ứng dụng đa dạng với cơ chế chọn đường đầy đủ và các khả năng mạng WAN được tích hợp trên các phần mềm Cisco ISO. Cisco IOS Firewall feature set có trong các bộ định tuyến dòng Cisco 1600, 2500, 2600 và 3600.

Các đặc điểm chính:

- Điều khiển truy cập dựa trên ngữ cảnh CBAC (Context-based access control): cung cấp bảo mật, lọc các ứng dụng cho lưu lượng IP, cung cấp các giao thức mới nhất.
- Java blocking - bảo mật chống lại các Java applet nguy hiểm, chỉ cho phép các applet từ các nguồn đáng tin cậy.

- Phát hiện và ngăn ngừa từ chối dịch vụ (Denial-of-service detection and prevention) để bảo mật các tài nguyên bộ định tuyến chống lại các tấn công thông thường.
- Cảnh báo thời gian thực (Real-time alert): cảnh báo trong trường hợp của các tấn công từ chối dịch vụ (denial-of-sevice) và các tình trạng đặc biệt khác.
- Theo dõi, kiểm tra (Audit trail): dò tìm người dùng truy cập bằng thời gian, địa chỉ nguồn và đích, cổng, tổng số byte được truyền đi.

Các máy chủ bảo mật

CiscoSecure ACS

CiscoSecure ACS là một họ các máy chủ AAA cung cấp TACACS+ hay các dịch vụ AAA trên cơ sở RADIUS. Các máy chủ này cho phép người cung cấp và khách hàng của họ tập trung các chính sách bảo mật, bao gồm điều khiển truy cập cá nhân qua các máy chủ truy cập mạng và tường lửa. Họ Cisco Secure cung cấp các sản phẩm từ mức đơn giản, dễ sử dụng (CPE cho các khách hàng nhỏ) đến các ứng dụng phức tạp hay các ứng dụng chuyên nghiệp như các nhóm quản trị mạng ...

Máy chủ bảo mật chuyển vùng toàn cầu của Cisco (Cisco Secure Global Roaming Server)

Cisco Secure Global Roaming Server (GRS) cho phép các nhà cung cấp dịch vụ cung cấp khác biệt dịch vụ lớn hơn bằng một mạng riêng ảo truy cập chuyển vùng toàn cầu (Global Roaming Access VPN). Máy chủ này có thể cung cấp quá trình hoạt động phức tạp của "proxy" và dịch các giao thức bảo mật TACACS+ và RADIUS.

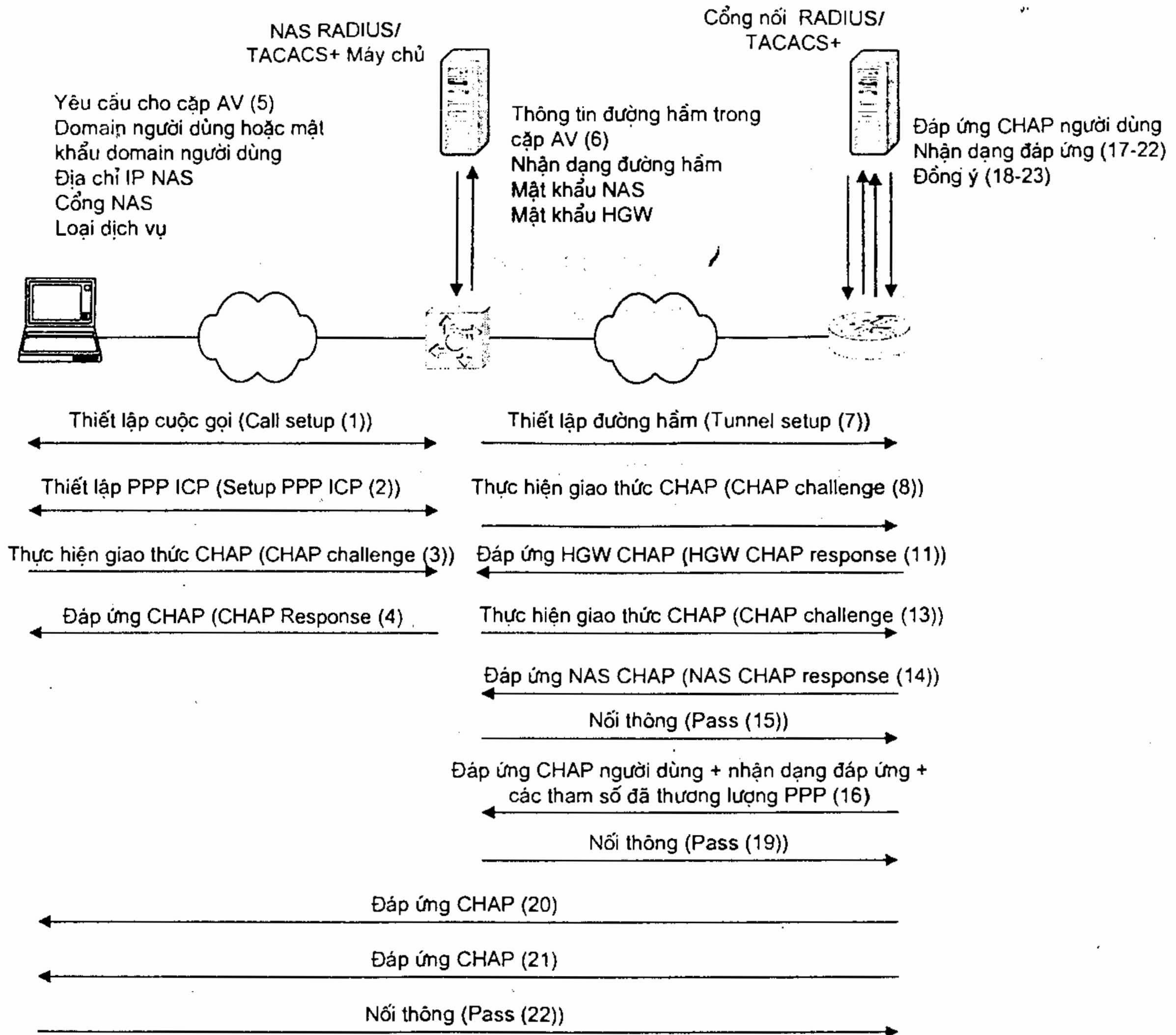
Điểm điều khiển người dùng

Điểm điều khiển người dùng USP (User Control Point) nối ACS và GRS với hệ thống tên miền DNS (Domain Name System) và giao thức cấu hình địa chỉ động DHCP (Dynamic Host Configuration Protocol) thành một sản phẩm chuyên nghiệp, kiến trúc tốt và độ tin cậy cao.

Hệ thống giám sát kiểm toán tích cực

Hệ thống Cisco NetRanger

Hệ thống dò tìm Cisco NetRanger cung cấp một phạm vi rộng lớn, thời gian thật của bảo mật mạng. Hệ thống NetRanger bao gồm hai thành phần: NetRanger Sensor được đặt tại điểm giám sát kết nối mạng (monitored network connection) và NetRanger Director được đặt trong máy chủ trung tâm Cisco Assure.



Hình 3.10: Sơ đồ luồng giao thức L2TP

Các đặc tính bảo mật của Cisco IOS

Các danh sách điều khiển truy cập chuẩn và mở rộng ACL (Standard and Extended Access Control Lists): cung cấp các điều khiển truy cập đến các đoạn mạng (segment) đặc biệt và xác định lưu lượng nào chuyển qua một đoạn mạng.

Khoá và chìa khoá - ACL động (Lock and Key - Dynamic ACLs): cho phép truy cập tạm thời qua các bộ định tuyến truy cập dựa trên xác thực người dùng (tên người dùng/mật khẩu).

Dịch địa chỉ mạng NAT (Network Address Tranlation): NAT làm tăng tính riêng tư của mạng bằng cách giấu đi các địa chỉ IP nội bộ không được đăng ký.

Các giao thức đường hầm của Cisco IOS

Chuyển tiếp lớp 2 - L2F (Layer 2 Forwarding)

Cisco đăng ký kỹ thuật mới này đến IETF nhằm đưa nó trở thành một tiêu chuẩn. Nó cung cấp các đặc điểm có thể mở rộng và độ tin cậy cao.

Giao thức định đường hầm lớp 2 - L2TP

Giao thức định đường hầm lớp 2 - L2TP (Layer 2 Tunneling Protocol) là một mở rộng của PPP. Đây là một bản thảo của tiêu chuẩn IETF xuất phát từ Cisco L2F và giao thức định đường hầm điểm-điểm của Microsoft. Tiêu chuẩn L2TP được hoàn tất vào cuối năm 1998. L2TP là một công nghệ chính của Cisco Access VPN cung cấp và phân phối phạm vi điều khiển bảo mật đầy đủ và các đặc điểm quản lý chính sách, bao gồm việc điều khiển bảo mật cho đầu cuối người dùng. Hình 3.10 mô tả thiết lập đường hầm đến cổng nối bằng cách sử dụng L2TP.

Bí mật dữ liệu (Data Privacy)

Cisco IPSec cung cấp tính riêng tư, toàn vẹn và xác thực cho các yêu cầu mạng mang tính thương mại, chủ yếu cho việc truyền dẫn các thông tin nhạy cảm trên các mạng công cộng. Công nghệ Cisco IPSec được cung cấp cho các hệ thống Windows 95, Windows NT 4.0, phần mềm Cisco IOS và Cisco PIX firewall. Cisco hỗ trợ các công nghệ sau như một giải pháp để đảm bảo tính riêng tư của dữ liệu:

- IPSec: sử dụng kỹ thuật mã hoá để cung cấp dữ liệu tin cậy, tính toàn vẹn và tính xác thực giữa các bên tham gia trong một mạng riêng.
- IKE: xác thực mỗi bên ngang hàng (peer) trong một tương tác IPSec, đàm phán chính sách bảo mật và điều khiển sự trao đổi của các khoá của phiên làm việc.
- Quản lý các chứng nhận (certificate management).

Các thành phần công nghệ IPSec bao gồm:

- Diffie-Helman, một phương pháp khoá công cộng cho trao đổi khoá. Tính chất này được sử dụng trong IKE để thiết lập các khoá phiên tạm thời.
- DES: sử dụng để mã hoá các gói dữ liệu.
- MD5/SHA (Message Digest 5/Secure Hash Algorithms) được sử dụng để xác thực gói dữ liệu.

IPSec trong phần mềm Cisco IOS cung cấp các tiêu chuẩn sau:

- Thuật toán mã hoá IPSec và IKE bao gồm:
  + DES-CBC với Explicit IV.
  + 40-bit DES-CBC với Explicit IV.

+ DES-CBC với Derived IV trong RFC 1829.

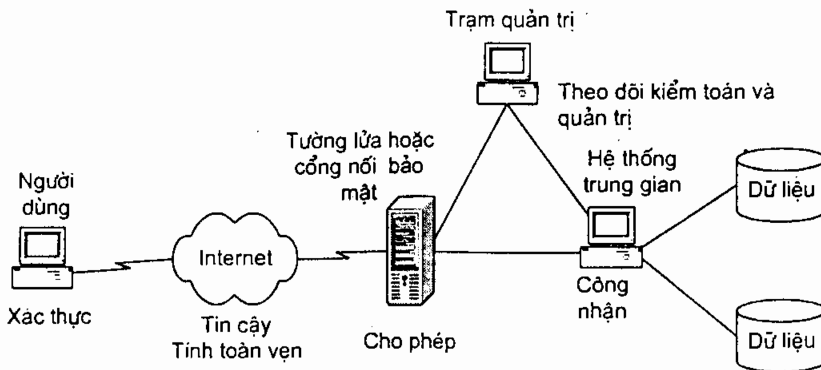
- Thuật toán xác thực:
  + HMAC-MD5.
  + HMAC-SHA.
  + Keyed MD5 trong RFC 1828.

CHƯƠNG 4

BẢO MẬT TRÊN MỘT MẠNG INTERNET VPN

Một trong những mối quan tâm chính của bất kỳ công ty nào là việc bảo mật dữ liệu của họ. Bảo mật dữ liệu chống lại các truy cập và thay đổi trái phép không chỉ là một vấn đề trên các mạng. Việc truyền dữ liệu giữa các máy tính hay giữa các mạng LAN với nhau có thể làm cho dữ liệu dễ bị tấn công do rình mò và dễ bị thâm nhập hơn là khi dữ liệu vẫn còn trên một máy tính đơn.

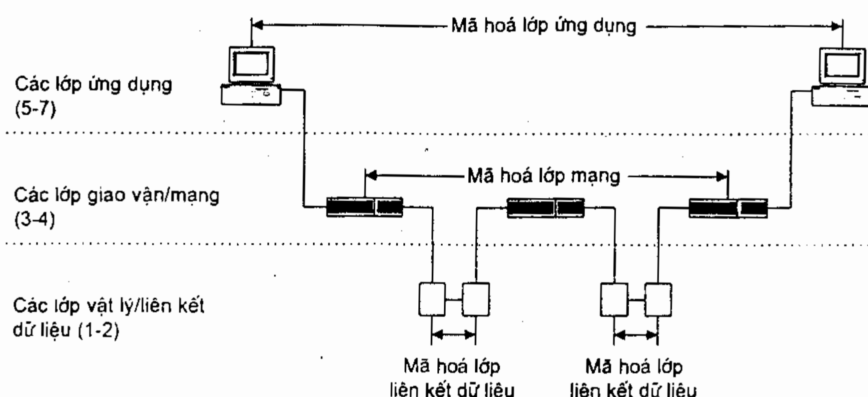
Một khung bảo mật thích hợp cho một tổ chức, cơ quan bao gồm 7 thành phần khác nhau: xác thực (authentication), tin cậy (confidentiality), tính toàn vẹn (integrity), cho phép (authorization), công nhận (nonrepudiation), quản trị (administration) và theo dõi kiểm toán (audit trail), theo hình 4.1.



Hình 4.1: Các thành phần của một hệ thống bảo mật

Bởi vì các giao thức TCP/IP không được thiết kế với dự phòng gắn liền cho bảo mật, nhiều hệ thống bảo mật khác nhau được phát triển cho các ứng dụng và lưu lượng (traffic) chạy trên mạng Internet. Phần mềm có nhiệm vụ chuẩn bị dữ liệu cho việc truyền trên một mạng cung cấp một số khả năng có thể áp dụng xác thực (authentication) và mã hoá (encryption). Những ứng dụng trên được thực hiện

trong một trong ba lớp: phần mềm ứng dụng (application software), chồng giao vận/mạng (network/transport stack), thiết bị liên kết dữ liệu (data link device) và ổ đĩa (driver) (hình 4.2). Một vài giao thức mật mã cho các ứng dụng bao gồm Secure MIME (S/MIME) và Pretty Good Privacy (PGP) cho e-mail và Secure Sockets Layer (SSL/TSL) và Secure HTTP (SHTTP) cho các ứng dụng Web. Nhưng cấu trúc quan trọng nhất của mạng VPN là xác thực và mã hoá ở lớp mạng và lớp liên kết dữ liệu.



Hình 4.2: So sánh mã hoá ở lớp mạng và lớp liên kết dữ liệu

4.1 Bảo mật trên mạng

Việc truyền dữ liệu trên các mạng IP có thể phải chịu nhiều mối nguy hiểm, trong đó có một số loại thông dụng: đánh lừa (spoofing), ăn cắp phiên (session hijacking), nghe trộm (sniffing / electronic eavesdropping) và tấn công chính giữa (the man-in-the-middle attack).

4.1.1 Đánh lừa

Giống như những mạng khác, các mạng IP sử dụng một địa chỉ số cho mỗi thiết bị được gắn vào mạng. Địa chỉ của nguồn và người nhận dự định được gắn vào trong mỗi gói dữ liệu được truyền đi trên mạng IP. Tấn công kiểu đánh lừa (spoofing) là việc một người tấn công có thể sử dụng địa chỉ IP của một ai đó và giả vờ trả lời người khác.

Sau khi một người tấn công (attacker) xác định được hai máy tính A và B đang truyền thông với nhau theo kiểu client/server, sẽ cố gắng thiết lập một kết nối với máy tính B theo cách mà B có thể tin rằng đó là kết nối với A, nhưng thực tế, kết nối là với máy tính của người tấn công.

Người tấn công thực hiện điều này bằng cách tạo ra một bản tin giả với địa chỉ nguồn là địa chỉ của A, yêu cầu một kết nối đến B. Khi B nhận được bản tin này, B sẽ đáp ứng bằng một xác thực (acknowlegment) có kèm theo những số tuần tự cho việc truyền dữ liệu với A. Những số tuần tự từ máy chủ B là duy nhất đối với kết nối giữa hai máy tính..

Để hoàn tất thiết lập phiên làm việc này giữa A và B, B sẽ mong chờ A xác thực con số tuần tự của B trước khi tiến hành bất kỳ sự trao đổi thông tin nào. Nhưng để cho người tấn công đóng vai bên A, anh ta phải đoán con số tuần tự mà B sẽ sử dụng và phải ngăn chặn bên A trả lời. Tuy nhiên, trong những hoàn cảnh cụ thể, không quá khó để có thể đoán được những con số tuần tự là gì.

Để giữ cho máy tính A không đáp ứng được bất kỳ việc truyền dữ liệu nào của B, người tấn công thường xuyên truyền một số lượng lớn các gói đến A, làm cho A bị quá tải để xử lý các gói này và ngăn chặn A khỏi việc đáp ứng các bản tin của B.

Spoofing tương đối dễ để bảo mật, bằng cách cấu hình các bộ định tuyến để loại bỏ những gói quay về nào mà bắt phải hình thành từ một máy tính trong mạng nội bộ, nhằm ngăn chặn bất kỳ máy tính bên ngoài nào khỏi việc lợi dụng các quan hệ của phiên làm việc trong mạng nội bộ. Nếu có những mối quan hệ vượt qua những giới hạn của mạng, như trên Internet, thì việc bảo mật chống lại các đánh lừa IP sẽ khó khăn hơn.

4.1.2 Ăn cắp phiên

Trong ăn cắp phiên, thay vì cố gắng khởi tạo một phiên làm việc bằng cách đánh lừa, người tấn công cố gắng tiếp quản một kết nối có sẵn giữa hai máy tính.

Đầu tiên, người tấn công điều khiển thiết bị mạng trên mạng LAN, có thể là một tường lửa hay là máy tính khác, do đó có thể giám sát kết nối. Qua việc giám sát kết nối giữa hai máy tính, người tấn công có thể xác định những số tuần tự được sử dụng bởi hai bên.

Sau khi giám sát kết nối và đã xác định được những con số tuần tự, người tấn công có thể tạo ra một lưu lượng, lưu lượng này xuất hiện để đến từ một trong các bên truyền thông, chiếm lấy phiên làm việc từ một trong những cá nhân tham gia. Giống như đánh lừa IP, người tấn công sẽ làm cho một trong các máy tính truyền thông bị quá tải với việc xử lý các gói tin. Do đó bị loại khỏi phiên truyền thông.

Những vấn đề gây ra bởi ăn cắp phiên chỉ ra rằng cần có một sự xác nhận thành viên trong một phiên làm việc. Sự thật là việc xác định người tham gia việc truyền thông không có nghĩa là có thể dựa trên IP để bảo đảm. Thậm chí các

phương pháp xác thực mạnh khác cũng không luôn luôn thành công trong việc ngăn chặn tấn công ăn cắp phiên. Biện pháp bảo mật duy nhất chống lại những tấn công đó là việc sử dụng rộng khắp các biện pháp mã hoá.

4.1.3 Nghe trộm

Nghe trộm là một cách tấn công khác xảy ra trên các mạng có môi trường dùng chung giống như những mạng IP trên cơ sở Ethernet (Ethernet-based IP), hầu hết những mạng LAN Ethernet, các gói sẵn sàng từ mỗi nút Ethernet trên mạng. Sự thoả thuận thông thường cho mỗi card giao tiếp mạng của mỗi nút là chỉ để lắng nghe và đáp ứng những gói mang địa chỉ đặc biệt đến nó. Điều này có vẻ dễ dàng, tuy nhiên để đặt nhiều card giao tiếp mạng Ethernet NIC (Network Interface Card) vào chế độ ngẫu nhiên, có nghĩa là phải thu thập mỗi gói chủ yếu trên đường dây. Một NIC như thế không thể được nhận ra từ một trạm khác trên mạng, vì NIC không làm gì đối với những gói mà nó thu thập được.

Một loại phần mềm gọi là đánh hơi (sniffer) có thể lợi dụng đặc điểm này của Ethernet. Những công cụ như vậy có thể ghi lại tất cả lưu lương mạng chuyển qua chúng. Và như thế, đó là một phần cần thiết của bộ các công cụ của bất kỳ sự chẩn đoán mạng nào làm việc với mạng Ethernet, cho phép xác định một cách nhanh chóng điều gì đang diễn ra trên một đoạn bất kỳ của mạng. Tuy nhiên, sniffer cũng là một công cụ mạnh mẽ để nghe lén. Ví dụ, một người tấn công có thể sử dụng một gói sniffer để ghi lại tất cả những gói đăng nhập vào mạng và sau đó sử dụng những thông tin đăng nhập này để xâm nhập vào một mạng mà anh ta không có quyền truy cập.

Nghe trộm cũng có thể được sử dụng để thu thập dữ liệu của công ty và những bản tin được truyền đi trên mạng, sau đó phân tích các lưu lượng mạng để biết được người nào đang truyền thông. Cơ chế xác thực mạnh sử dụng mật khẩu một lần (one-time password) hay sử dụng thẻ bài (token) là một cách để giữ cho một người dùng nào đó sử dụng sniffer không thể sử dụng lại mật khẩu mà người dùng đó đang giữ một cách trái phép. Mã hoá dữ liệu cũng là một cách để bảo mật dữ liệu chống lại việc nghe trộm, mặc dù đây không phải là giải pháp hữu hiệu, người tấn công có những tài nguyên để lưu giữ lại các dữ liệu được mã hoá và cố gắng giải mã những bản tin đó ngoại tuyến.

Giám sát vật lý của các mạng là một cách tốt để làm giảm nguy cơ ăn trộm, bởi các sniffer phải được gắn một cách vật lý vào mạng để giữ lấy các gói. Mặc dù ở một số máy tính chạy trên Unix, có thể dễ dàng kiểm tra khi nào NIC được cài đặt để chạy trong chế độ ngẫu nhiên.

4.1.4 Tấn công ngay chính giữa

Mặc dù dường như rõ ràng là việc sử dụng những kỹ thuật mã hoá để bảo mật và xác thực dữ liệu được chuyển đi trong các gói IP là một giải pháp cho những nguy cơ đến bảo mật IP đã được đề cập, nhưng mã hoá không phải là một giải pháp không có lỗi. Chúng ta vẫn cần quản lý một cách cẩn thận hệ thống mã hoá để bảo mật chống lại những tấn công khác, như tấn công ngay chính giữa (the man-in-the-middle attack).

Để sử dụng mã hoá, trước tiên phải trao đổi các khoá mã hoá. Nhưng việc trao đổi những khoá không được bảo mật trên mạng có thể dễ dàng làm thất bại toàn bộ mục đích của hệ thống bởi vì những khoá đó có thể bị giữ lại và đưa dữ liệu đến một kiểu tấn công khác đó là bị tấn công ngay chính giữa. Một người tấn công sử dụng phương pháp đánh lừa, ăn cắp phiên và nghe trộm có thể thu được một số trao đổi khoá như vậy. Người đó có thể nhanh chóng tạo ra khoá riêng cho mình trong tiến trình, vì thế trong khi người dùng tin rằng mình đang truyền thông với một khoá của một thành viên, thì trên thực tế người dùng đó đang dùng một khoá đã bị tấn công ngay chính giữa.

4.2 Hệ thống xác thực

Xác thực (authentication), là một phần không thể thiếu được của kiến trúc bảo mật của một mạng VPN. Trừ khi hệ thống của chúng ta có thể xác thực đúng một cách tin cậy những người dùng, những dịch vụ và các mạng, chúng ta có thể không cần phải điều khiển truy cập đến các tài nguyên dùng chung và giữ những người dùng bất hợp pháp (unauthorized), không được truy cập vào mạng.

Xác thực được dựa trên ba thuộc tính sau: cái gì ta có (một khoá hay một card token); cái gì chúng ta biết (một mật khẩu) hay cái gì nhận dạng chúng ta (giọng nói, quét võng mạc, dấu vân tay,...). Những chuyên gia về bảo mật cho rằng một giải pháp xác thực đơn, ví dụ như một mật khẩu, thì sẽ không đủ mạnh để bảo mật hệ thống. Thay vào đó, họ đề nghị xác thực sâu hơn, hay việc sử dụng ít nhất hai trong số các thuộc tính được nêu ở trên cho việc xác thực.

Sự đa dạng của các hệ thống VPN hiện nay dựa trên các phương pháp xác thực khác nhau hay là sự kết hợp giữa chúng. Có thể phân loại theo cách sau: mật khẩu truyền thống, mật khẩu một lần (S/Key) hay các hệ thống mật khẩu khác (PAP, CHAP, TACACS và RADIUS), hay dựa trên cơ sở phần cứng (token, smart card, PC card) và các nhận diện sinh trắc học (biometric ID) như dấu vân tay, giọng nói, quét võng mạc,...

4.2.1 Mật khẩu truyền thống

Người ta công nhận rằng, các loại xác thực đơn giản, như số nhận dạng ID của người dùng, mật khẩu không đủ mạnh cho việc bảo mật truy cập mạng. Mật khẩu có thể bị đón bắt và giữ lấy trong suốt quá trình truyền dữ liệu của mạng. Thậm chí khi người dùng cẩn thận trong việc bảo mật mật khẩu của họ, thì họ có thể không nhận ra rằng các dịch vụ Internet khác không cung cấp bảo mật cho các mật khẩu của họ.

Hệ thống mật khẩu một lần có thể được xem là phương pháp tốt đối với một số vấn đề xảy ra xung quanh việc sử dụng mật khẩu truyền thống.

4.2.2 Mật khẩu một lần

Một cách để ngăn chặn việc sử dụng trái phép các mật khẩu bị giữ lại là ngăn không cho chúng được dùng trở lại, bằng cách yêu cầu một mật khẩu mới cho mỗi phiên làm việc mới.

Những hệ thống này, trong đó S/Key là một ví dụ điển hình, loại bỏ khó khăn của người dùng khi luôn luôn phải chọn một mật khẩu mới cho mỗi phiên làm việc kế tiếp bằng cách tạo ra một cách tự động một danh sách mật khẩu có thể chấp nhận được cho người dùng. Ví dụ IETF thực hiện tiêu chuẩn S/Key theo RFC 2289.

S/Key dùng một nhóm thông qua bí mật, được tạo ra bởi người dùng cho việc tạo ra một tuần tự của các mật khẩu một lần OTP (One-Time Password). Nhóm thông qua bí mật của người dùng không bao giờ di chuyển vượt quá máy tính nội bộ và không di chuyển trên mạng, do đó nó không là đối tượng cho các cuộc tấn công. Cũng thế, vì một OTP khác nhau được tạo ra cho riêng mỗi phiên làm việc, do đó một mật khẩu đã bị chiếm giữ không thể được sử dụng lại thành công, vì thế nó không mang lại cho các tin tặc bất kỳ thông tin nào về mật khẩu kế tiếp sẽ được sử dụng.

Một chuỗi tuần tự các OTP được tạo ra bởi việc áp dụng một hàm băm bảo mật (secure hash function) đa thời gian đến các bản tin đã được tạo ra trong bước khởi tạo. Nói một cách khác, OTP đầu tiên được tạo ra bởi việc chuyển bản tin tóm tắt (message digest) qua hàm băm N lần, trong đó N được chỉ định bởi người dùng, OTP kế tiếp được tạo ra bởi việc chuyển bản tin tóm tắt qua hàm băm N-1 lần và cứ như thế cho đến khi OTP thứ N được tạo ra.

Khi một người dùng cố gắng đăng nhập vào mạng, máy chủ của mạng có khả năng S/Key bảo mật thâm nhập mạng, đưa ra một con số thách đố gồm một con số và một chuỗi các ký tự, được gọi là seed. Để đáp ứng, người dùng nhập vào con số thách đố và seed kèm theo nhóm thông qua bí mật riêng của mình vào phần mềm

phát S/Key chạy trên máy tính của mình. Phần mềm này sau đó kết hợp nhóm thông qua bí mật với seed và nhắc một hàm băm hoạt động lặp lại với số lần lặp lại phụ thuộc vào con số thách đố. Kết quả của việc tính toán là một mật khẩu một lần bao gồm 6 ký tự.

OTP được gửi đến các máy chủ mạng, cũng lặp lại hàm băm và so sánh kết quả với OTP đã được lưu giữ được dùng cho hầu hết các đăng nhập hiện tại. Nếu phù hợp, người dùng sẽ được phép đăng nhập vào mạng, con số thách đố này bị làm giảm đi, OTP cuối cùng được giữ lại cho lần đăng nhập kế tiếp.

Giống như S/Key, các hệ thống OTP yêu cầu phần mềm của máy chủ được cập nhật để thực hiện các tính toán được yêu cầu và do đó mỗi máy tính từ xa có một bản sao chép của phần mềm dành cho khách hàng (client). Nhược điểm của các hệ thống này là khó có thể quản trị những danh sách mật khẩu cho một số lượng lớn các người dùng.

4.2.3 Các hệ thống khác

4.2.3.1 Giao thức xác thực mật khẩu PAP

Giao thức xác thực mật khẩu PAP (Password Authentication Protocol) được thiết kế một cách đơn giản cho một máy tính tự xác thực đến một máy tính khác khi giao thức điểm-điểm (Point-to-Point Protocol) được sử dụng làm giao thức truyền thông. PAP là một giao thức bắt tay hai chiều; đó là, máy tính chủ tạo kết nối gửi một nhận dạng người dùng và mật khẩu kép (password pair) đến hệ thống đích mà nó cố gắng thiết lập một kết nối và sau đó hệ thống đích xác thực rằng máy tính đó được xác thực đúng và được chấp nhận cho việc truyền thông.

Xác thực PAP có thể được dùng khi bắt đầu của kết nối PPP, cũng như trong suốt một phiên làm việc của PPP để xác thực lại kết nối.

Khi một kết nối PPP được thiết lập xác thực PAP có thể được diễn ra trên kết nối đó. Điểm ngang hàng gửi một nhận dạng người dùng và mật khẩu trong một sự rõ ràng đến bộ xác thực cho đến khi bộ xác thực chấp nhận kết nối hay kết nối bị hủy bỏ. PAP không bảo mật bởi vì thông tin xác thực được truyền đi rõ ràng và không có gì bảo mật chống lại tấn công trở lại hay lặp lại quá nhiều bởi những người tấn công nhằm cố gắng đoán ra một mật khẩu đúng hay một đoán ra một cặp nhận dạng người dùng.

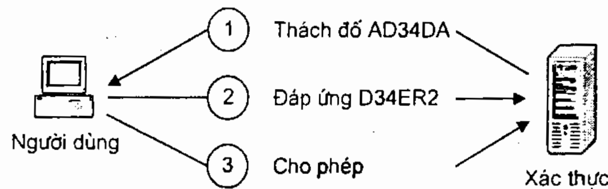
4.2.3.2 Giao thức xác thực yêu cầu bắt tay CHAP

Giao thức xác thực yêu cầu bắt tay CHAP (Challenge Handshake Authentication Protocol) được thiết kế cho việc sử dụng tương tự như PAP nhưng là một phương pháp bảo mật hơn đối với xác thực các kết nối PPP. CHAP là một giao

thức bắt tay ba chiều. Giống như PAP, CHAP có thể dùng khi bắt đầu kết nối PPP và sau đó được lặp lại sau khi kết nối được thiết lập xong.

CHAP được xem như một giao thức bắt tay ba chiều bởi vì nó bao gồm ba bước để thực hiện một kết nối được kiểm tra đúng sau khi kết nối được khởi tạo đầu tiên hay tại bất kỳ thời điểm nào sau khi kết nối được thiết lập và được kiểm tra đúng. Thay vì dùng một mật khẩu hai bước đơn giản hay tiến trình chấp thuận giống như đã dùng trong PAP, CHAP sử dụng một hàm băm một chiều (one-way hashing function) theo kiểu tương tự như được dùng bởi S/Key. Được trình bày như sau đây (hình 4.3):

1. Bộ xác thực gửi một bản tin thách đố (challenge message) đến máy tính ngang cấp (peer).
2. Máy tính ngang cấp tính toán một giá trị sử dụng một hàm băm một chiều và gửi trả lại cho bộ xác thực.
3. Máy tính xác thực (authenticator) có thể đáp ứng chấp nhận nếu tương ứng với giá trị mong muốn.



Hình 4.3: Hệ thống đáp ứng thách đố dùng CHAP

Tiến trình này có thể được lặp lại tại bất kỳ thời điểm nào trong suốt liên kết PPP để đảm bảo rằng kết nối không được nắm quyền hay bị suy yếu trong bất kỳ trường hợp nào. Không giống như PPP được điều khiển bởi phía client, máy chủ điều khiển quá trình xác thực lại CHAP.

CHAP cũng có thể gỡ bỏ khả năng mà người tấn công có thể cố gắng đăng nhập trên cùng một kết nối.

Khi xác thực CHAP sai, máy chủ được yêu cầu hủy kết nối. Điều này gây khó khăn cho việc đoán mật khẩu của người tấn công bởi vì không thể cố gắng có những suy đoán mới trong một kết nối đơn.

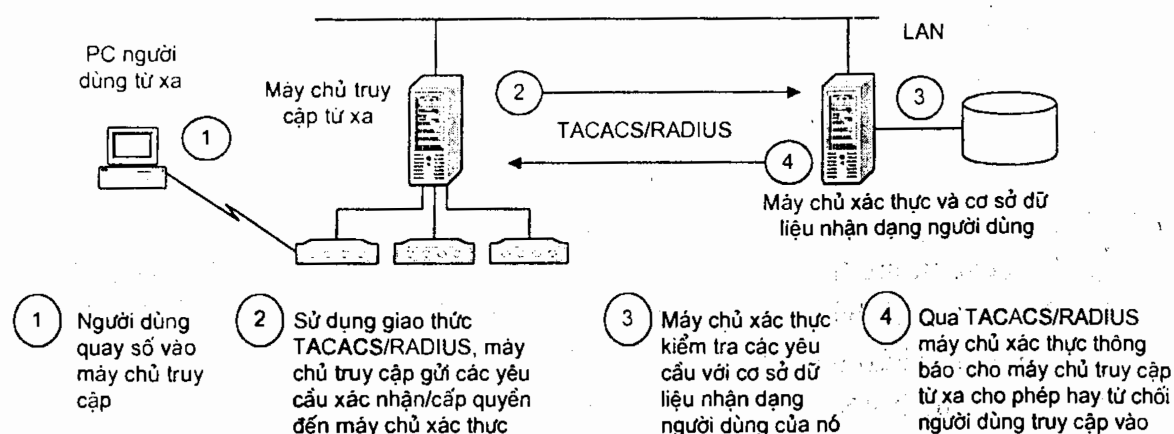
PAP và CHAP đều có những nhược điểm. Cả PAP & CHAP đều phụ thuộc vào một mật khẩu bí mật phải được lưu giữ trên một máy tính của người dùng ở xa và máy tính nội bộ. Nếu bất kỳ máy tính nào chịu sự điều khiển của một kẻ tấn công mạng, sau đó mật khẩu bí mật được thay đổi. Cũng vậy, với xác thực CHAP

hay PAP, không thể đăng ký chỉ định những đặc quyền truy cập mạng khác nhau đến những người dùng ở xa khác nhau sử dụng cùng một host - máy chủ ở xa.

Mặc dù CHAP là một phương pháp mạnh hơn PAP cho việc xác thực quay số người dùng, nhưng CHAP có thể không đáp ứng những yêu cầu mang tính mở rộng của những công ty hay các tổ chức lớn. Cho dù nó không truyền bất kỳ những bí mật nào qua một mạng, nhưng nó cũng yêu cầu một số lớn các bí mật dùng chung chạy qua hàm băm. Các tổ chức với nhiều người dùng quay số phải duy trì những chính sách rất lớn để có thể đáp ứng tất cả họ.

4.2.3.3 Hệ thống điều khiển truy cập bộ điều khiển truy cập đầu cuối - TACACS

TACACS (Terminal Access Controller Access Control System) là một trong những hệ thống được phát triển để không chỉ cung cấp cơ chế xác thực, mà còn để thêm vào hai chức năng 2A trong việc bảo mật truy cập từ xa, đó là: cho phép (authorization) và tính cước (accouting). Không như những mối quan hệ ngang cấp được thiết kế trong PAP và CHAP, TACACS được thiết kế có chức năng như một hệ thống client/server, trong đó mang tính mềm dẻo hơn, đặc biệt trong việc quản lý bảo mật mạng. Trung tâm hoạt động của TACACS và RADIUS là một máy chủ xác thực (authentication server) (hình 4.4).



Hình 4.4: Các máy chủ xác thực cấp quyền truy cập từ xa

Một máy chủ xác thực TACACS giữ các yêu cầu từ phần mềm client xác thực được cài đặt tại một gateway hay tại một điểm truy cập mạng (network entry point). Máy chủ xác thực duy trì một cơ sở dữ liệu của các nhận dạng người dùng, mật khẩu, PIN và các khoá bí mật được sử dụng để đạt được hay từ chối các yêu cầu truy cập mạng. Tất cả xác thực (authentication), cấp quyền (authorization) và

dữ liệu cước được hướng đến máy chủ trung tâm khi một người dùng cố gắng đăng nhập vào mạng.

Một ưu điểm của TACACS là nó hoạt động như một máy chủ proxy đối với những hệ thống xác thực khác, ví dụ như: một tên miền bảo mật trong Win NT, NDS, dựa trên Unix; hay những hệ thống bảo mật khác (các hệ thống sử dụng thẻ bài). Các khả năng proxy cũng làm cho việc một client chia sẻ dữ liệu bảo mật của VPN với một ISP được dễ dàng hơn, điều này cần thiết khi một VPN là nguồn xuất; ISP chạy một máy chủ proxy để điều khiển việc truy cập quay số dựa trên các quyền truy cập được điều hành bởi hiệp hội khách hàng trên máy chủ bảo mật riêng của họ. Nhưng việc truyền các gói xác thực giữa máy chủ chính và máy chủ proxy qua một mạng công cộng có độ rủi ro nhất định. Mã hoá RADIUS và TACACS được dựa trên các khoá tĩnh, tên người dùng, mật khẩu và thông tin máy chủ xác thực được gửi trên một gói đơn làm cho chúng dễ được sử dụng hơn nếu như bị lưu giữ.

4.2.3.4 Dịch vụ xác thực người dùng quay số từ xa - RADIUS

RADIUS (Remote Authentication Dial-In User Service) cũng sử dụng một kiểu client/server để chứng nhận một cách bảo mật và quản trị các kết nối mạng từ xa của các người dùng với các phiên làm việc. RADIUS giúp cho việc điều khiển truy cập dễ quản lý hơn và nó có thể hỗ trợ các kiểu xác thực người dùng khác nhau bao gồm PAP và CHAP.

Kiểu RADIUS client/server dùng một máy chủ truy cập mạng NAS (Network Access Server) để quản lý các kết nối người dùng. Mặc dù NAS hoạt động như một máy chủ cung cấp truy cập mạng nhưng nó cũng hoạt động như một client đối với RADIUS (hình 4.4). NAS có trách nhiệm chấp nhận các yêu cầu kết nối của người dùng, thu thập các thông tin nhận dạng người dùng, mật khẩu đồng thời chuyển các thông tin này một cách bảo mật đến máy chủ RADIUS. Máy chủ RADIUS trở lại chế độ xác thực để chấp nhận hay từ chối cũng như khi có bất kỳ dữ kiệu cấu hình nào được yêu cầu để NAS cung cấp các dịch vụ đến đầu cuối người dùng.

Các client RADIUS và máy chủ truyền thông với nhau một cách bảo mật bằng việc sử dụng các bí mật dùng chung cho việc xác thực và mã hoá đối với việc truyền mật khẩu người dùng.

RADIUS tạo một cơ sở dữ liệu đơn và tập trung của người dùng và các dịch vụ, một đặc điểm quan trọng cơ bản đối với các mạng bao gồm các dải modem (modem bank) lớn và có nhiều hơn một máy chủ truyền thông từ xa (remote communication server). Với RADIUS, thông tin người dùng được lưu giữ tại một nơi là máy chủ RADIUS nhằm quản lý việc xác thực người dùng và các truy cập

đến các dịch vụ từ một site. Bởi vì với bất kỳ thiết bị nào hỗ trợ RADIUS có thể là RADIUS client, một người dùng ở xa sẽ đạt được quyền truy cập đến các dịch vụ như nhau từ bất kỳ một máy chủ truyền thông nào đang truyền thông với máy chủ RADIUS.

4.2.4 Các hệ thống phần cứng cơ bản

4.2.4.1 Smart Card và PC Card

Card thông minh (Smart Card) là thiết bị có kích thước giống như một thẻ tín dụng, bao gồm: một bộ vi xử lý được gắn chặt vào card và bộ nhớ. Một thiết bị cuối Smart Card hay bộ đọc tương đương cho Smart Card được yêu cầu để giao tiếp với Smart Card, vì thế thông tin mới có thể được trao đổi như mong muốn. Nhiều bộ đọc kiểu này hiện nay được dùng với một ổ đĩa mềm PC hay được tích hợp vào bàn phím làm cho việc sử dụng chúng với PC đơn giản hơn nhiều so với trước đây.

Smart Card có thể lưu giữ một khoá riêng của người dùng cùng với bất kỳ ứng dụng nào được cài đặt nhằm đơn giản hoá tiến trình xác thực, đặc biệt đối với các người dùng di động. Một số Smart Card hiện nay gồm một bộ đồng xử lý mã hoá và giải mã làm cho việc mã hoá dữ liệu dễ dàng hơn và nhanh hơn các loại cũ. Nhiều nhà phát triển phần mềm ứng dụng các chuẩn hoá APIS như CryptoAPI cho việc dùng với Windows, nhằm làm cho các Smart Card và PC phù hợp với nhau.

Các hệ thống chứng nhận điện tử đơn giản nhất yêu cầu người dùng nhập vào một số nhận diện cá nhân PIN để hoàn tất tiến trình xác thực. Trong một số trường hợp, PIN được lưu trữ trên Smart Card và việc sử dụng PIN để xác thực người dùng được kiểm tra một cách tự động bởi Smart Card trước khi diễn ra bất cứ trao đổi nào khác với phần còn lại của hệ thống. Khi PIN không được lưu giữ trên card thì phương pháp này có thể không có đủ bảo mật, vì thế, các hệ thống đầu cuối mạnh hơn kết hợp thông tin được lưu trên Smart Card với các thông tin về sinh trắc học (biometric). Để dùng những hệ thống này, các bộ đọc card bao gồm một thiết bị kiểm tra sinh học, ví dụ như máy quét vân tay... Dữ liệu được quét sau đó được so sánh với dữ liệu đã được lưu trên Smart Card.

Có một kiểu khác cho việc sử dụng card điện tử, được dùng để gắn vào PC, ví dụ như PC Card. PC Card còn được gọi là PCMCIA Card, đó là các bo mạch nhỏ có thể được gắn vào các khe đặc biệt bên trong máy tính để bàn, đặc biệt là máy tính xách tay, để cung cấp các chức năng mở rộng. Những card này có thể cung cấp một số chức năng như Smart Card nhưng bị hạn chế là chỉ dùng được với các PC có các khe PCMCIA. Điều này làm cho chúng kém linh động hơn so với các thiết bị truy cập khác đang được sử dụng. Tuy nhiên, PCMCIA Card có những ưu điểm là bộ nhớ lớn, cho phép lưu trữ các tệp tin lớn hơn được dùng cho mục đích xác thực.

4.2.4.2 Các thiết bị thẻ bài (Token Devices)

Các hệ thống thẻ bài cơ bản thường được dựa trên các phần cứng riêng biệt dùng để hiển thị các mã nhận dạng (passcode) thay đổi mà người dùng sau đó phải nhập vào máy tính để thực hiện việc xác thực.

Cơ chế hoạt động của xác thực thẻ bài cơ bản như sau: một bộ xử lý bên trong thẻ bài lưu giữ một tập hợp các khoá mã hoá bí mật được dùng để phát các mã nhận dạng một lần. Các mã nhận dạng này được chuyển đến một máy chủ bảo mật trên mạng, máy chủ này kiểm tra tính hợp lệ và cấp quyền truy cập cho người dùng. Sau khi các mã được lập trình, không có người dùng nào hay quản trị mạng nào có quyền truy cập đến chúng.

Trước khi các người dùng được cho phép xác thực chính họ, các thiết bị thẻ bài yêu cầu một PIN, sau đó sử dụng một trong ba cơ chế khác nhau để xác định người dùng là ai.

- Cơ chế thông dụng nhất là đáp ứng thách đố (challenge- response) (hình 4.3) trong đó máy chủ bảo mật phát ra một con số ngẫu nhiên khi người dùng đăng nhập vào mạng. Một số thách đố (challenge) xuất hiện trên màn hình của người dùng, sau đó, người dùng nhập vào các con số trong thẻ bài. Thẻ bài mã hoá con số thách đố này với khoá bí mật của nó và hiển thị kết quả lên màn hình LCD, sau đó, người dùng nhập kết quả đó vào trong máy tính. Trong khi đó, máy chủ mã hoá con số thách đố với cùng một khoá và nếu như hai kết quả này phù hợp, người dùng sẽ được phép vào mạng.
- Một cơ chế khác là sử dụng sự đồng bộ thời gian (time synchcronization). Ở đây, thẻ hiển thị một số được mã hoá với khoá bí mật mà khoá này sẽ thay đổi cứ mỗi 60 giây. Người dùng được nhắc cho con số khi cố gắng để đăng nhập vào máy chủ. Bởi vì các đồng hồ trên máy chủ và thẻ được đồng bộ, cho nên, máy chủ có thể xác thực người dùng bằng cách giải mã con số thẻ (Token number) và so sánh các kết quả.
- Cơ chế thứ ba là đồng bộ sự kiện (event synchcronization), một biến đồng bộ thời gian. Ở đây, một bộ đếm ghi lại số lần vào mạng được thực hiện bởi người dùng. Sau mỗi lần vào mạng, bộ đếm được cập nhật và một mã nhận dạng khác được tạo ra cho lần đăng nhập kế.

4.2.5 Hệ thống sinh trắc học

Hệ thống sinh trắc học (biometric) phụ thuộc vào việc sử dụng một dấu vết cá nhân duy nhất để xác định người dùng. Các kỹ thuật sinh trắc học đánh giá các đặc tính, tính chất của con người như: vân tay, giọng nói, dấu võng mạc ... Nhưng các hệ

thống chưa được sử dụng trong nhiều thực tiễn bởi vì giá thành đắt và các hệ thống bảo mật này thường là tất cả trong một, làm cho chúng khó khăn trong việc giao tiếp với các hệ thống khác.

Một trong những kỹ thuật phát triển mạnh mẽ nhất là việc quét vân tay. Các máy quét vân tay với giá cả chấp nhận được, được kết hợp vào bàn phím của PC vào khoảng năm 1998. Một máy quét trên một con chip được phát triển cho phép quét dấu vân tay kết hợp một cách trực tiếp vào một Smart Card.

Một hệ thống chuẩn đoán khuôn mặt có thể hoạt động trên một PC với giá thấp, trong đó, camera có độ phân giải thấp thường được dùng cho các cuộc hội nghị truyền hình. Một cơ sở dữ liệu trung tâm lưu giữ những hình ảnh của các người dùng hợp lệ và so sánh hình ảnh được truyền từ camera với hình ảnh đã được lưu giữ để cấp quyền truy cập.

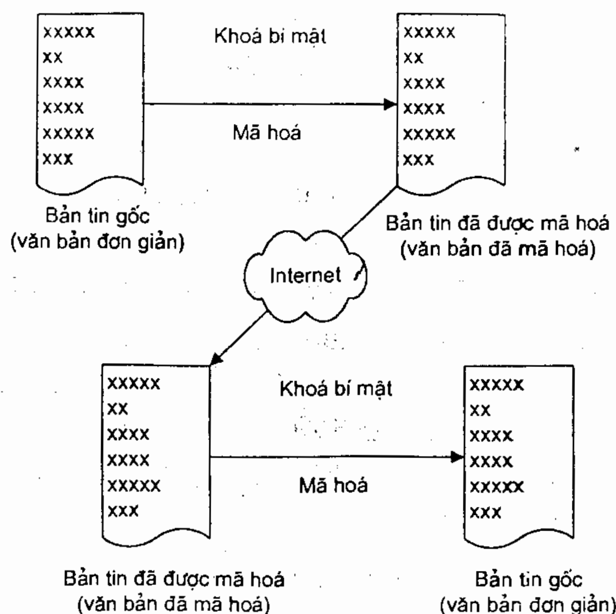
Mặc dù việc sử dụng các hệ thống sinh trắc học xuất hiện ngày càng tăng nhưng vẫn thiếu một tiêu chuẩn đặt ra cho các giao diện chương trình ứng dụng API (Application Programming Interfaces) cho hầu hết các phương pháp sinh trắc học gây ra khó khăn khi sẵn sàng kết hợp sinh trắc học vào các hệ thống bảo mật sẵn có.

4.3 Mật mã

4.3.1 Thế nào là mã hoá?

Mã hoá được dựa trên hai thành phần: đó là một thuật toán và một khoá. Một thuật toán mã hoá là một chức năng toán học nối phần văn bản hay các thông tin dễ hiểu với một chuỗi các số gọi là khoá để tạo ra một văn bản mật mã khó hiểu. Mặc dù có một vài thuật toán mã hoá đặc biệt không sử dụng khoá có sẵn nhưng với các thuật toán sử dụng các khoá thì đặc biệt quan trọng hơn. Mã hoá trên một hệ thống khoá cơ bản cung cấp hai ưu điểm quan trọng: một là bằng việc dùng một khoá có thể sử dụng cùng một thuật toán để truyền thông với nhiều người; tất cả những gì phải làm là sử dụng một khoá khác cho mỗi thành viên tương ứng. Thứ hai, nếu như bản tin được mã hoá bị bẻ gãy, chỉ cần chuyển một khoá mới để bắt đầu mã hoá bản tin đó lại mà không cần phải đổi một thuật toán mới để thực hiện quá trình đó.

Số khoá mà thuật toán có thể cung cấp phụ thuộc vào số bit trong khoá. Ví dụ: một khoá dài 8 bit cho phép có 256 số kết nối có thể hay còn gọi là khoá. Số khoá càng lớn thì khả năng một bản tin đã được mã hoá bị bẻ khoá càng thấp. Mức độ khó phụ thuộc vào chiều dài của khoá.



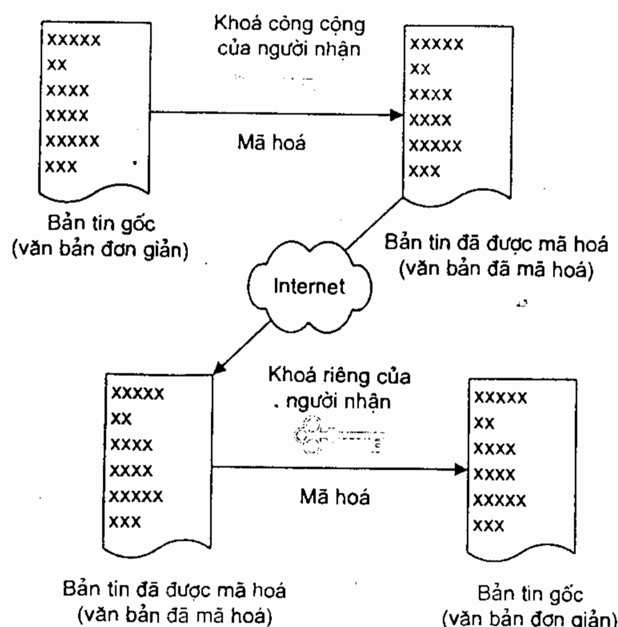
Hình 4.5: Mã hoá đối xứng dùng một khoá bí mật đơn để mã hoá và giải mã

Hình thức cũ nhất của mã hoá dạng khoá cơ bản được gọi là mã hoá khoá bí mật (secret key) hay còn gọi là mã hoá đối xứng (symmetric). Trong cơ chế này, cả người gửi lẫn người nhận đều chiếm giữ cùng một khoá; có nghĩa là, cả hai bên có thể mã hoá và giải mã dữ liệu với khoá đó. Nhưng mã hoá đối xứng xuất hiện một số các trở ngại: ví dụ, cả hai bên phải đồng ý trên một khoá bí mật được chia sẻ. Nếu như chúng ta có nhiều sự trao đổi thì chúng ta phải giữ dấu của n khoá bí mật với mỗi khoá được dùng cho mỗi sự trao đổi. Nếu như sử dụng cùng một khoá cho nhiều trao đổi thì người nhận sẽ có khả năng đọc thư của người khác (hình 4.5).

Cơ chế mã hoá đối xứng cũng có một vấn đề với việc xác thực bởi vì đặc điểm nhận dạng của một bản tin gốc hay người nhận không thể chứng minh được. Do hai bên cùng chiếm giữ một khoá giống nhau nên đều có thể tạo và mã hoá và cho là người khác gửi bản tin đó. Điều này gây ra sự mơ hồ về tác giả của bản tin đó. Để giải quyết tình huống này, người ta sử dụng mã hoá khoá công cộng.

4.3.2. Thế nào là mã hoá khoá công cộng?

Mã hoá khoá công cộng (Public key) được dựa trên ý niệm của khoá đôi. Một phần của khoá đôi, khoá riêng (Private key) chỉ được biết đến bởi người thiết kế; phần khác là khoá công cộng có thể được công bố một cách rộng rãi nhưng vẫn được kết hợp với người sở hữu. Các khoá đôi có một đặc điểm duy nhất là dữ liệu đã mã hoá với một khoá có thể được giải mã với một khoá khác trong cùng một cặp (hình 4.6).



Hình 4.6: Sử dụng một cặp khoá để mã hoá và giải mã bản tin

Những khoá này có thể được dùng trong hai cách khác nhau: cung cấp bản tin một cách tin cậy và chứng minh sự tin cậy của một bản tin gốc. Trong trường hợp đầu tiên, người gửi sử dụng khoá công cộng của người dự định nhận để mã hoá một bản tin, do đó, nó sẽ vẫn còn tin cậy cho đến khi được giải mã bởi người nhận với khoá riêng. Trong trường hợp thứ hai, người gửi mã hoá một bản tin bằng cách sử dụng một khoá riêng (khoá mà chỉ có người gửi truy cập được).

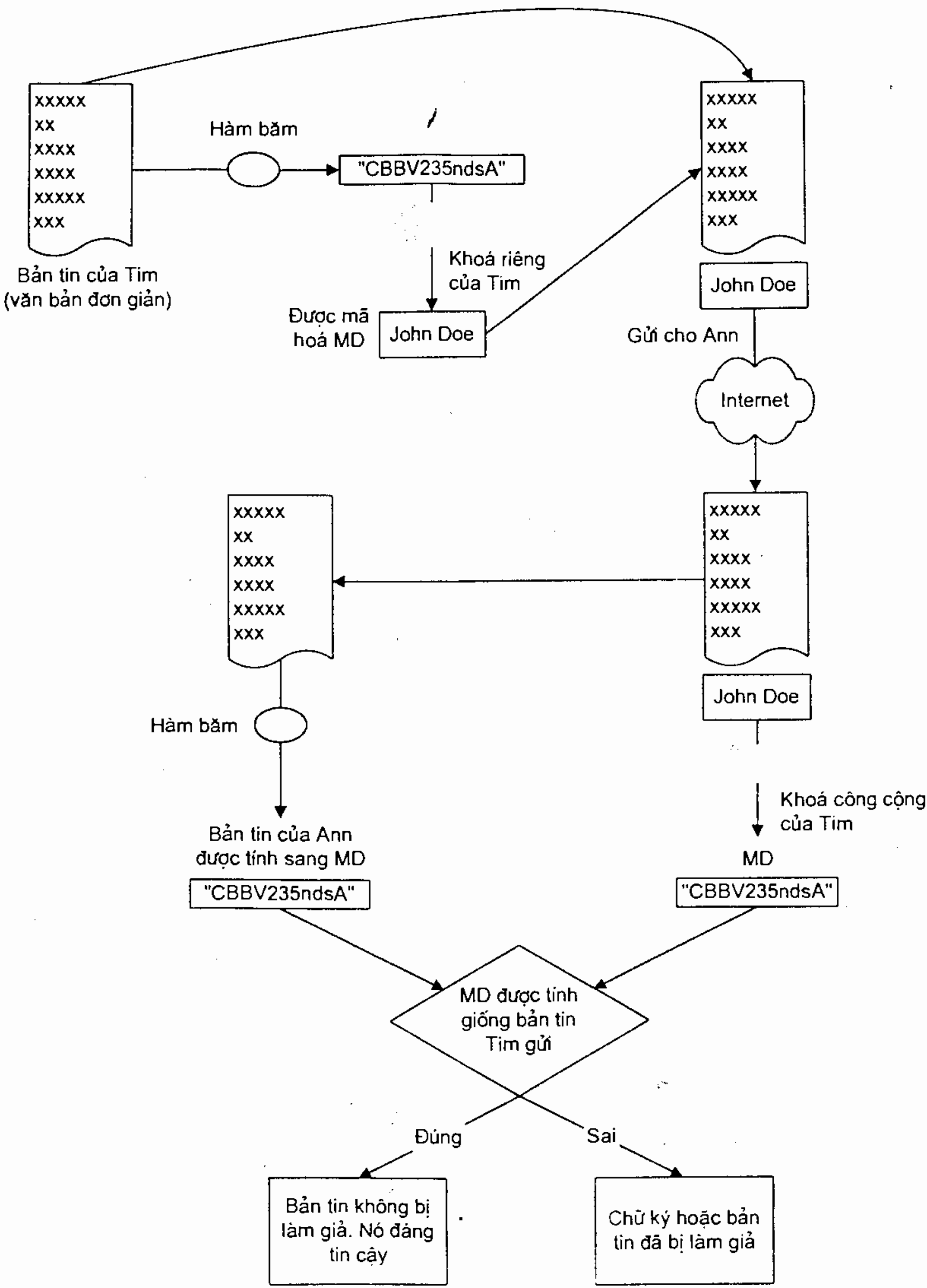
Ưu điểm

- Khoá công cộng của khoá đôi có thể được phân phát một cách sẵn sàng mà không sợ rằng điều này làm ảnh hưởng đến việc sử dụng các khoá riêng. Không cần phải gửi một bản sao chép khoá công cộng cho tất cả các đáp ứng mà chúng ta có thể lấy nó từ một máy chủ được duy trì bởi một công ty hay là nhà cung cấp dịch vụ.
- Cho phép xác thực nguồn phát của bản tin.

Ví dụ minh họa: hình 4.7

Việc sử dụng các thuật toán mã hoá khoá công cộng để mã hoá các bản tin tương đối chậm. Vì thế, một giải pháp được đưa ra là bản tin tóm tắt (Message Digest) có thể được mã hoá và sau đó được dùng như chữ ký điện tử. Các thuật toán mã hoá sử dụng phương pháp này được biết đến là các hàm băm một chiều. Hàm băm một chiều không dùng một khoá, nó chỉ đơn giản là một công thức để

chuyển đổi một bản tin có chiều dài bất kỳ thành một chuỗi đơn các số gọi là một bản tin tóm tắt.



Hình 4.7: Xác nhận một chữ ký số

Khi dùng một hàm băm 16-bit, văn bản được xử lý sẽ tạo ra 16 bit và kết quả là một chuỗi, ví dụ như: "CBBV235ndsA63D67". Và mỗi bản tin tạo ra một bản tin tóm tắt ngẫu nhiên.

Các bản tin tóm tắt có thể chứng tỏ sự hữu dụng như một bộ xác định rằng dữ liệu không bị thay đổi, tuy nhiên, chữ ký điện tử được xem là tin cậy hơn nhiều.

Một vấn đề với phương pháp này là khi một bản sao của đoạn văn bản được gửi đi như một phần của bản tin và do đó, sự riêng tư không còn được duy trì. Nếu như muốn duy trì sự riêng tư của dữ liệu thì nên mã hoá bản tin. Nhưng để làm giảm ảnh hưởng đến các phần đầu, nên dùng một thuật toán đối xứng với một khoá bí mật.

4.3.3 Hai phương pháp khoá công cộng quan trọng

4.3.3.1 Kỹ thuật Diffie - Hellman

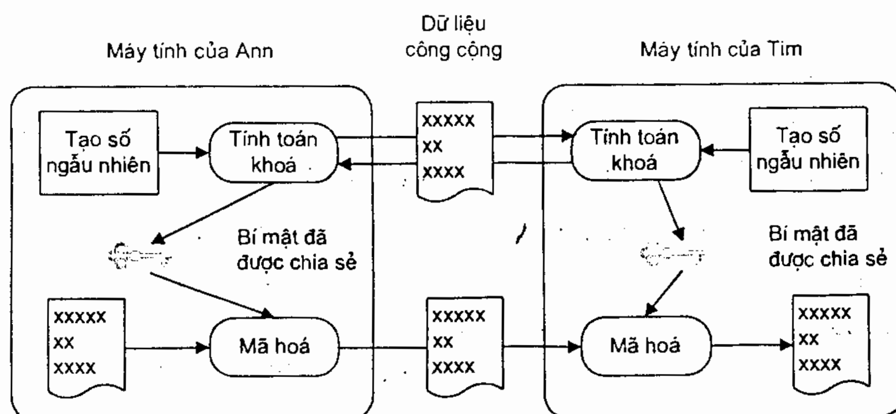
Kỹ thuật Diffie - Hellman là thuật toán mã hoá khoá công cộng thực tế đầu tiên. Trong thực tế, kỹ thuật này được ứng dụng rất nhiều cho việc quản lý khoá.

Cơ chế làm việc: hai bên trao đổi có thể sử dụng kỹ thuật Diffie - Hellman để tạo ra một giá trị bí mật dùng chung mà sau đó có thể được dùng như một khoá chung cho một thuật toán mã hoá khoá bí mật (xem hình 4.8).

Trong hình 4.8, Tim và Ann đều tạo ra một con số ngẫu nhiên trên mỗi máy tính riêng của họ; hai số ngẫu nhiên này trở thành các khoá riêng của họ. Để truyền thông, trước tiên họ trao đổi một số dữ liệu chung được xem là khoá chung. Sau đó, Ann ghép khoá riêng của mình với khoá công cộng của Tim để tính toán một giá trị bí mật được chia sẻ và Tim cũng làm như vậy.

Nếu như có một người khác có được các giá trị khoá công cộng này thì không thể dễ dàng tính toán ra được giá trị bí mật ngẫu nhiên từ đó. Điểm quan trọng của thuật toán Diffie - Hellman là cả Ann và Tim đều kết thúc với một kết quả giống nhau và không một ai khác có thể dễ dàng tính ra kết quả tương tự từ thông tin công cộng sẵn có.

Trong kỹ thuật Diffie - Hellman, cả Ann và Tim đều đồng ý một con số cơ sở riêng biệt và con số này được chọn là khoá riêng của mỗi cá nhân, một số lượng lớn các con số ngẫu nhiên trở thành khoá công cộng, ví dụ (B)A cho Ann. Khoá công cộng của Tim có thể là (B)T. Khi Tim nhận được khoá công cộng của Ann, (B)A, anh ta có thể tạo thành khoá riêng (BA)T để lấy bí mật được chia sẻ. Khi Ann nhận được khoá công cộng của Tim, cô ta có thể tạo thành khoá riêng (BT)A mà khoá này thì giống hệt kết quả mà Tim đã tính toán.



Hình 4.8: Kết quả của kỹ thuật Diffie - Hellman chia sẻ bí mật

Kỹ thuật Diffie - Hellman có thể đặc biệt có ích cho việc tạo ra các khoá của các phiên làm việc tạm thời. Các phiên này được dùng chỉ bởi các bên liên quan trong suốt một sự trao đổi thông tin và bị xóa đi sau đó. Việc sử dụng một khoá mới cho mỗi phiên làm giảm nguy cơ ảnh hưởng đến bảo mật mạng.

4.3.3.2 Mật mã khoá công cộng RSA

Kỹ thuật khoá công cộng RSA khoá công cộng có tên bắt nguồn từ ba nhà phát triển là: Ron Rivest, Adir Shamir và Leonard Adelman. Bảo mật của kỹ thuật này được dựa trên thực tế là có thể tương đối dễ dàng để nhân A và B được kết quả là C, nhưng không dễ dàng khi biết C lại có thể suy ra A và B khi A và B là những số tương đối lớn. Kỹ thuật này tạo ra các khoá công cộng phù hợp với các khoá riêng đặc biệt. Điều này tạo cho RSA những ưu điểm của việc cho phép người giữ một khoá riêng mã hoá dữ liệu với khoá đó, vì thế, bất kỳ người nào với một bản sao của khoá công cộng đều có thể giải mã nó sau đó.

Khoá RSA bao gồm ba giá trị số đặc biệt được sử dụng trong các cặp để mã hoá và giải mã dữ liệu. Khoá công cộng RSA gồm một giá trị khoá công cộng (thường là 317 hay 65.537) và một mạch toán modulus (mạch lấy giá trị tuyệt đối). Modulus là sản phẩm của hai số lớn chính được chọn một cách ngẫu nhiên, được liên kết một cách toán học đến khoá công cộng đã được chọn. Khoá riêng được tính toán từ hai số chính phát ra từ Modulus và giá trị khoá công cộng.

4.3.4 Chọn lựa các giải pháp mã hoá

Không có một hệ thống mã hoá nào là lý tưởng cho tất cả các tình trạng mạng. Bảng 4.1 mô tả ưu và nhược điểm của một số kiểu mã hoá.

Bảng 4.1: Các ưu và nhược điểm của các hệ thống mã hoá

Kiểu mã hoá	Ưu điểm	Nhược điểm
Khoá bí mật (đối xứng)	- Nhanh. - Có thể được bổ sung một cách dễ dàng trong phần cứng.	- Các khoá giống nhau. - Khó khăn cho việc phân phối khoá. - Không hỗ trợ các chữ ký điện tử
Khoá công cộng	- Sử dụng hai khoá khác nhau. - Tương đối dễ phân phối các khoá. - Cung cấp tính toàn vẹn không từ chối qua các chữ ký điện tử.	- Chậm và đòi hỏi tính toán nhiều.

Khi chọn lựa một thuật toán phù hợp để sử dụng, nguyên tắc chung là xác định dữ liệu của chúng ta dễ bị ảnh hưởng ra sao và bao lâu thì dữ liệu cần phải được bảo mật. Khi đã chỉ ra được, lựa chọn một thuật toán mã hoá và chiều dài khoá thích hợp với yêu cầu đó.

Bảng 4.2: So sánh chi phí và thời gian cần thiết để bẻ các khoá có độ dài khác nhau

Giá (USD)	Chiều dài bit của khoá				
	40	56	64	80	128
100,000	2 giây	35 giờ	1 năm	70000 năm	10^{19} năm
1,000,000	2 giây	3,5 giờ	37 ngày	7000 năm	10^{18} năm
100 triệu	2 miligiây	2 phút	9 giờ	70 năm	10^{16} năm
1 tỷ	2 miligiây	13 giây	1 giờ	7 năm	10^{15} năm
100 tỷ	2 microgiây	1 giây	32 giây	24 ngày	10^{11} năm

Bảng 4.3: Chiều dài của khoá bí mật và khoá công cộng đối với các mức bằng nhau của việc bảo mật

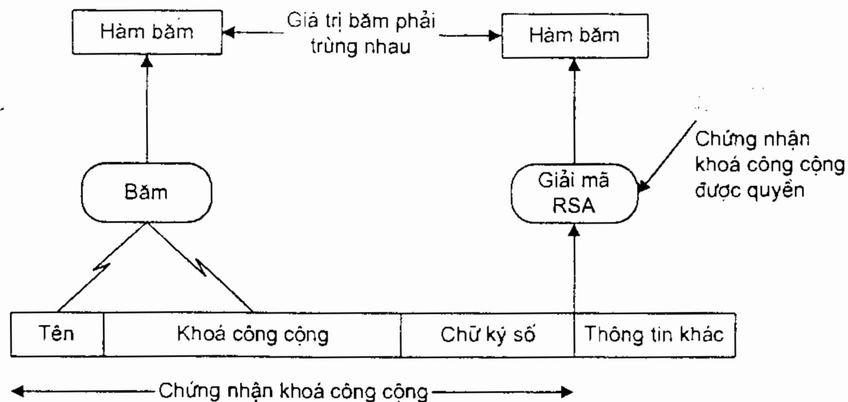
Chiều dài của khoá bí mật	Chiều dài khoá công cộng
56 bit	384 bit
64 bit	512 bit
80 bit	768 bit
112 bit	1,792 bit
128 bit	2,304 bit

4.3.5 Cấu trúc của một khoá công cộng

4.3.5.1 Chứng nhận khoá công cộng

Thông tin nhận dạng của Tim: tên, tổ chức, địa chỉ
Phát hành chữ ký số cấp quyền và thông tin nhận dạng
Khoá công cộng của Tim
Ngày hợp lệ của nhận dạng số này
Loại chứng nhận
Số chứng nhận của nhận dạng số

Hình 4.9: Nội dung của một chứng nhận khoá công cộng



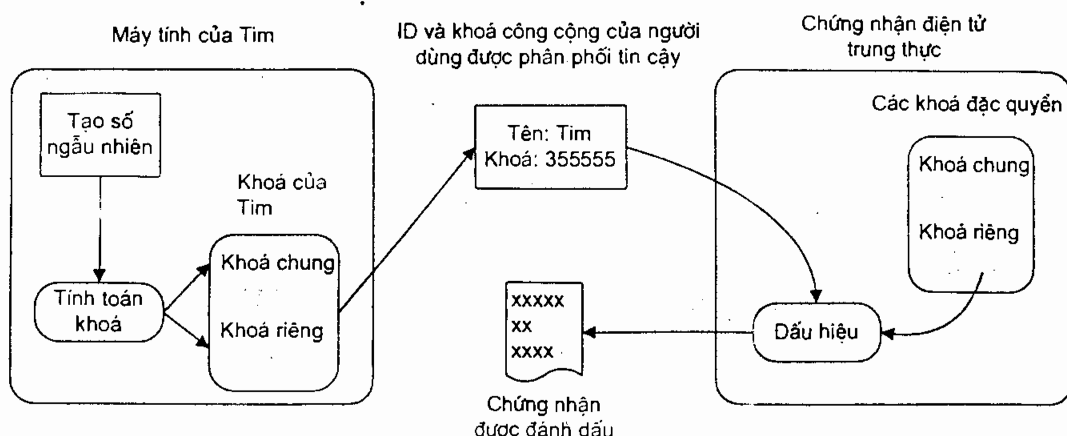
Hình 4.10: Chứng nhận khoá công cộng hợp lệ

Chứng nhận khoá công cộng (Public key Certificate) trên hình 4.9 là các khối dữ liệu được sắp xếp một cách đặc biệt cho biết giá trị của một khoá công cộng, tên của người sở hữu khoá và một chữ ký điện tử của cơ quan cung cấp, được gọi là một chứng nhận điện tử CA (Certificate Authority). Những chứng nhận này được dùng để xác định người sở hữu của một khoá công cộng cụ thể. Và khi có một bản sao chép khoá công cộng của người có quyền, có thể dùng khoá đó để kiểm tra những chứng nhận mà nó đã đăng ký (hình 4.10). Bất kỳ phần mềm mã hoá nào cũng phải có một bản sao chép khoá công cộng của CA để kiểm tra một chữ ký điện tử.

Tiêu chuẩn chính cho các chứng nhận là X.509 - ITU đưa ra các dạng thức của chứng nhận và các điều kiện để tạo và sử dụng các chứng nhận này.

4.3.5.2 Tạo ra khoá công cộng

Có hai cách để tạo ra một cặp khoá công cộng, đó là: một số hệ thống phát ra các khoá trên máy chủ tùy thuộc vào người giữ khoá và một số hệ thống khác tạo ra các khoá như một phần của việc tạo ra các chứng nhận.



Hình 4.11: Tạo một khoá công cộng

Thứ nhất: tạo các khoá tùy thuộc vào người giữ các khoá (khoá sở hữu), được mô tả trong hình 4.11. Người dùng tạo ra một cặp khoá công cộng, giữ lại khoá riêng và phát khoá công cộng đến CA để tạo ra một chứng nhận.

Thứ hai: có một CA tạo một đôi khoá công cộng (khoá đặc quyền), phát ra chứng nhận đã được đăng ký và chuyển cả khoá đôi và chứng nhận đó đến người dùng.

Bảng 4.4: Các ưu điểm và nhược điểm của các phương án tạo khoá

Tạo các khoá sở hữu	Tạo các khoá đặc quyền
+ Các người dùng phải chuyển khoá đến CA. + Khoá riêng không cần được sao chép lại. + Khoá chữ ký cá nhân không lấy trở lại.	+ Yêu cầu ít bước thực hiện hơn cho người dùng. + Khoá riêng có thể được dự phòng. + Việc tạo khoá có thể được chia sẻ giữa các người dùng.

4.3.5.3 Phân phối chứng nhận và khoá

Cho dù các khoá công cộng dễ phân phối hơn các khoá bí mật, nhưng vẫn cần các phương tiện đáng tin cậy để chuyển các khoá công cộng. Nếu không, nó sẽ dễ

có khả năng chịu một tấn công ngay chính giữa cản trở một cặp khoá công cộng của người dùng trong việc chia sẻ thông tin riêng. Phương pháp chung cho việc chuyển các khoá công cộng là thông qua các chứng nhận điện tử hay các chứng nhận khoá công cộng.

Các chứng nhận cung cấp một giải pháp bảo mật cho việc phân phối các khoá công cộng qua môi trường điện tử. Sau khi các chứng nhận được tạo ra, vấn đề kế tiếp là chuyển các chứng nhận này đến các máy có nhu cầu. Các kỹ thuật thường được sử dụng trong thực tế là phân phối trong suốt (Transparent distribution) và phân phối liên tác (Interactive distribuiton).

Phân phối trong suốt gồm các máy chủ thư mục hay các giao thức trao đổi khoá. Các giao thức thư mục (Directory Protocol) cho việc chuyển các chứng nhận khoá công cộng được phát triển từ X.500. Mặc dù có một số lớn các thư mục chính cho các chứng nhận có thể được dựa trên X.500, nhưng có một giao thức đáng lưu ý khác cũng được sử dụng đó là LDAP (Lightweight Directory Access Protocol) được sử dụng nhiều hơn trên các mạng TCP/IP.

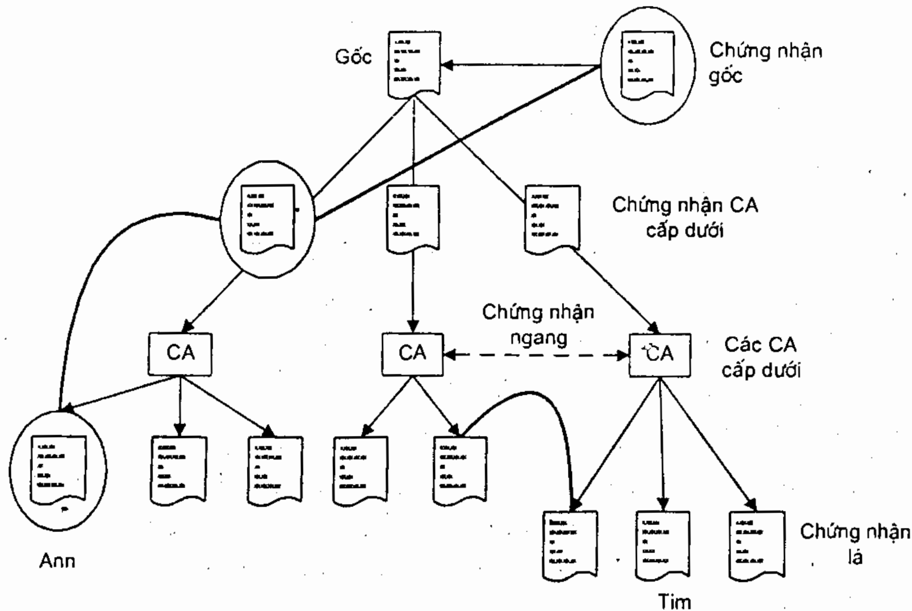
Phân phối liên tác bao gồm các yêu cầu e-mail, sự truy cập đến website, hay các yêu cầu sử dụng giao thức Finger. Nhiều hệ thống e-mail hỗ trợ cho mã hoá, cung cấp một phương pháp để gửi kèm một chứng nhận trong bản tin được gửi đi. Trong một số trường hợp, một máy chủ xác thực có thể được cấu hình để chấp nhận các yêu cầu e-mail cho các chứng nhận.

4.3.5.4 Chứng nhận đặc quyền CA

Có hai kiểu khác nhau của các hệ thống phân phối chứng nhận đó là: một hệ thống có cài đặt phân cấp và một trang web tin cậy, nhưng chúng ta chỉ tập trung vào các hệ thống có phân cấp.

Trong một hệ thống phân cấp, một khoá công cộng gốc (root public key), có tại đỉnh của hệ thống phân cấp được sử dụng để đánh dấu cho tất cả các quyền ở mức cao, khoá gốc này có thể thuộc về một cơ quan chính phủ (ví dụ như DoD hay U.S Postal Service). Các CA ở mức thấp hơn trong hệ thống phân cấp, có các chứng nhận được đánh dấu bởi các CA ở mức cao và sẽ đánh dấu cho các CA mức thấp hơn chúng trong hệ thống phân cấp và tương tự như thế cho đến mức thấp nhất của hệ thống.

Để xác thực tính hợp lệ một chứng nhận của người dùng một cách đầy đủ, chúng ta phải xác thực tất cả các CA trong một hệ thống phân cấp giữa CA nội bộ với nơi phát CA. Điều này có thể bao gồm việc di chuyển lên trên một nhánh trong một hệ thống phân cấp CA (CA hierarchy) lên đến gốc và xuống một nhánh khác (hình 4.12).



Hình 4.12: Phân cấp của chứng nhận đặc quyền

Trong thực tế, các hệ thống CA không sâu. Các hệ thống này không có nhiều mức và mức con. Vì thế thời gian được yêu cầu để xác thực một khoá ngắn và không tác động một cách nghiêm trọng đến việc sử dụng mạng. Thực ra, đối với một mạng VPN, một công ty liên doanh có thể phục vụ như CA mà không yêu cầu kết nối đến bất kỳ một hệ thống phân cấp quốc gia hay quốc tế nào.

Nhưng nếu như mạng VPN được mở rộng cho các đối tác kinh doanh, trở thành một mạng Extranet, thì chúng ta phải tùy thuộc vào một số hệ thống phân cấp CA cho việc xác định các chứng nhận. Nếu như số người dùng ngoài mạng của mạng VPN Extranet của bạn tương đối ít, họ có thể sử dụng CA bên trong của bạn.

Việc sử dụng một hệ thống phân cấp CA có thể không có vấn đề gì trong thời điểm hiện tại do số lượng các CA tương đối nhỏ và các hệ thống này không sâu. Nhưng khi có càng nhiều chứng nhận được tạo ra và có càng nhiều chứng nhận được sử dụng thì số lượng các CA nhất định gia tăng và những hệ thống này sẽ phức tạp hơn.

Các chứng nhận đặc quyền có thể cung cấp nhiều cách để ngắn mạch việc xác nhận phân cấp bằng cách chứng nhận ngang. Nếu hai CA đồng ý chứng nhận lẫn nhau, một yêu cầu cho việc xác thực tính hợp lệ một chứng nhận được phát bởi một CA có thể được chuyển một cách trực tiếp đến CA khác mà không gồm phần còn lại của hệ thống phân cấp CA.

Một cách phân phối các khoá công cộng tốt hơn và tin cậy hơn là phát ra một quyền chứng nhận (certificate authority). Một chứng nhận đặc quyền sẽ chấp nhận khoá công cộng đó, kèm theo một số chứng cứ của nét nhận dạng người dùng và phục vụ như một bộ lưu trữ của một chứng nhận điện tử mà người khác có thể yêu cầu để xác thực khoá công cộng của người dùng, các chứng nhận điện tử hoạt động giống như khoá công cộng.

Các chứng nhận đặc quyền như VeriSign, CyberTrust và Nortel, phát ra các chứng nhận điện tử (digital certificate). Một chứng nhận bao gồm tên của người giữ, tên của chứng nhận đặc quyền, một khoá công cộng cho mã hoá, giải mã và một giới hạn thời gian sử dụng của chứng nhận, thường là 6 tháng hay một năm.

Một chứng nhận điện tử có thể được phát ra ở 1 trong 4 lớp, nhằm chỉ ra người giữ đó được xác thực ở mức độ nào. Lớp 1 là lớp dễ đạt được nhất bởi vì các phép kiểm tra là ít nhất trên nền của người dùng; chỉ có tên và địa chỉ e-mail là được xác thực. Đối với chứng nhận lớp 2, quyền phát ra (issuing authority) kiểm tra một giấy phép lái xe, số chứng minh và ngày sinh. Các người dùng sử dụng lớp 3 có thể chờ đợi một thẻ tín dụng kiểm tra sử dụng một dịch vụ như Equifax để thêm vào thông tin yêu cầu cho một chứng nhận lớp 2. Một chứng nhận lớp 4 bao gồm thông tin về tình trạng cá nhân trong một tổ chức, nhưng những yêu cầu xác thực tính hợp lệ cho những chứng nhận này vẫn chưa được kết thúc bởi các nơi phát ra chứng nhận.

Các CA cũng có trách nhiệm duy trì và tạo tính sẵn sàng cho một danh sách hủy bỏ chứng nhận CRL (Certificate Revocation List), danh sách này cho phép các người dùng biết những chứng nhận nào không còn được sử dụng, CRL không bao gồm các chứng nhận hết hạn, bởi vì mỗi chứng nhận có một thời gian hạn định được xây dựng. Tuy nhiên, các chứng nhận có thể bị hủy bỏ do chúng bị mất, hay bị lấy trộm, hay do một người nào đó rời khỏi công ty.

Nếu một công ty tạo CA bên trong riêng, nó phải được chuẩn bị để tạo ra các khoá đôi, phát các chứng nhận và quản lý những khoá và các chứng nhận này. Cài đặt như trên bao gồm các dịch vụ sau:

- Chứng nhận khoá công cộng.
- Lưu trữ chứng nhận.
- Hủy bỏ chứng nhận.
- Khoá dự phòng và phục hồi.
- Hỗ trợ việc không từ chối chữ ký điện tử .
- Tự động cập nhật các khoá đôi và các chứng nhận.
- Quản lý lịch sử khoá.
- Hỗ trợ cho chứng nhận ngang .
- Phần mềm phía client.

CHƯƠNG 5

GIAO THỨC IPSEC

Các giao thức nguyên thủy TCP/IP không bao gồm các đặc tính bảo mật vốn có. Trong giai đoạn đầu của Internet khi mà người dùng thuộc các trường đại học và các viện nghiên cứu thì vấn đề bảo mật dữ liệu không phải là vấn đề quan trọng như bây giờ khi mà các ứng dụng thương mại có mặt khắp nơi trên Internet.

Để thiết lập tính bảo mật trong IP ở cấp độ gói, IETF đã đưa ra họ giao thức IPSec. Họ giao thức IPSec đầu tiên, cho xác thực, mã hoá các gói dữ liệu IP, được chuẩn hoá thành các RFC từ 1825 đến 1829 vào năm 1995. Họ giao thức này mô tả kiến trúc cơ bản của IPSec bao gồm 2 loại tiêu đề được sử dụng trong gói IP. Gói IP là đơn vị dữ liệu cơ sở trong mạng IP. IPSec định nghĩa 2 loại tiêu đề cho các gói IP để điều khiển quá trình xác thực và mã hoá: một là xác thực tiêu đề IP-AH (IP Authentication Header) điều khiển việc xác thực và hai là bọc gói bảo mật tải ESP (Encapsulating Security Payload) cho mục đích mã hoá.

IPSec được phát triển nhắm vào họ giao thức IP kế tiếp là IPv6, nhưng do việc chấp nhận IPv6 còn lâu và cần thiết cho việc bảo mật các gói IP nên IPSec đã được thay đổi cho phù hợp với IPv4. Việc hỗ trợ cho IPSec chỉ là tuỳ chọn của IPv4 nhưng đối với IPv6 thì có sẵn IPSec.

5.1 Dạng thức của IPSec

Hoạt động của IPSec ở mức cơ bản đòi hỏi phải có các phần chính đó là:

- Kết hợp bảo mật SA (Security Association).
- Xác thực tiêu đề AH (Authentication Header).
- Bọc gói bảo mật tải ESP (Encapsulating Security Payload).
- Chế độ làm việc.

5.1.1 Kết hợp bảo mật SA

Để hai bên có thể truyền dữ liệu đã được bảo mật (dữ liệu đã được xác thực hoặc được mã hoá hoặc cả hai) cả hai bên phải cùng thống nhất sử dụng giải thuật mã hoá, làm cách nào để chuyển khoá và chuyển khoá nếu như cần. Cả hai bên cũng cần thỏa thuận bao lâu thì sẽ thay đổi khoá một lần. Tất cả các thỏa thuận trên là do SA đảm trách. Việc truyền thông giữa bên gửi và bên nhận đòi hỏi ít nhất một SA và có thể đòi hỏi nhiều hơn vì mỗi giao thức IPSec đòi hỏi phải có một SA cho riêng nó. Do đó một gói được xác thực đòi hỏi một SA, một gói được mã hoá cũng yêu cầu phải có một SA. Thậm chí nếu cùng dùng chung một giải thuật cho xác thực và mã hoá thì cũng cần phải có 2 SA khác nhau do sử dụng những bộ khoá khác nhau.

Một IPSec SA mô tả các vấn đề sau:

- Giải thuật xác thực sử dụng cho AH và khoá của nó.
- Giải thuật mã hoá ESP và khoá của nó.
- Dạng thức và kích thước của bộ mật mã sử dụng trong giải thuật mã hoá.
- Giao thức, giải thuật, khoá sử dụng cho việc truyền thông.
- Giao thức, giải thuật mã hoá, khoá sử dụng cho việc truyền thông riêng.
- Bao lâu thì khoá được thay đổi.
- Giải thuật xác thực, kiểu, chức năng sử dụng trong ESP và khoá được sử dụng bởi giải thuật đó.
- Thời gian sống của khoá.
- Thời gian sống của SA.
- Địa chỉ nguồn SA.

Có thể xem SA như một kênh bảo mật thông qua một mạng công cộng đến một người hay một nhóm làm việc cụ thể.

5.1.2 Xác thực tiêu đề AH

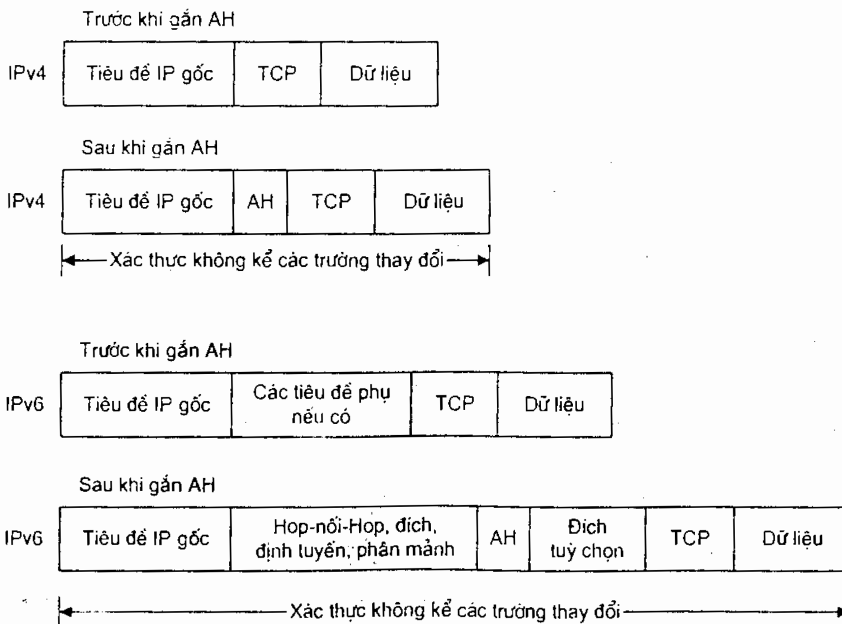
Trong hệ thống IPSec, xác thực tiêu đề AH (Authentication Header) được sử dụng cho các dịch vụ xác thực. AH được chèn vào giữa tiêu đề IP và nội dung phía sau (hình 5.3), không làm thay đổi nội dung của gói dữ liệu.

Xác thực tiêu đề gồm 5 trường: trường tiêu đề kế tiếp (Next Header Field), chiều dài tải (Payload Length), chỉ số tham số bảo mật SPI (Security Parameter Index), số tuần tự (Sequence Number), dữ liệu xác thực (Authentication Data). Hai khái niệm mới trong AH đó là SPI mang ý nghĩa chỉ ra thiết bị nhận gói biết họ

giao thức bảo mật mà phía gửi dùng trong truyền thông, hai là dữ liệu xác thực mang thông tin về giải thuật mã hoá được định nghĩa bởi SPI.

HMAC kết hợp với MD5, HMAC kết hợp với SHA-1 là giải thuật mã hoá được chọn làm những phương thức mặc định cho việc tính toán tổng kiểm tra (checksum). Các mặc định này là kết quả của những thay đổi IPSec để cải thiện cơ chế xác thực bởi vì mặc định trước đó MD5 được phát hiện là không tránh được các tấn công đụng độ.

Thủ tục sử dụng cho các phương thức này (HMAC-MD5 hay HMAC-SHA-1) giống nhau. Tuy nhiên SHA-1 có chức năng băm hơn MD5. Trong cả hai trường hợp, giải thuật hoạt động trên những khối dữ liệu 64 byte. Phương thức HMAC-MD5 sinh ra bộ xác thực 128 bit trong khi HMAC-SAH-1 sinh ra bộ xác thực 160 bit. Bởi vì chiều dài mặc định của xác thực được định nghĩa trong AH chỉ có 96 bit nên các giá trị xác thực sinh ra phải được chia nhỏ trước khi lưu vào trong trường xác thực của AH.



Hình 5.3: Xác thực tiêu đề

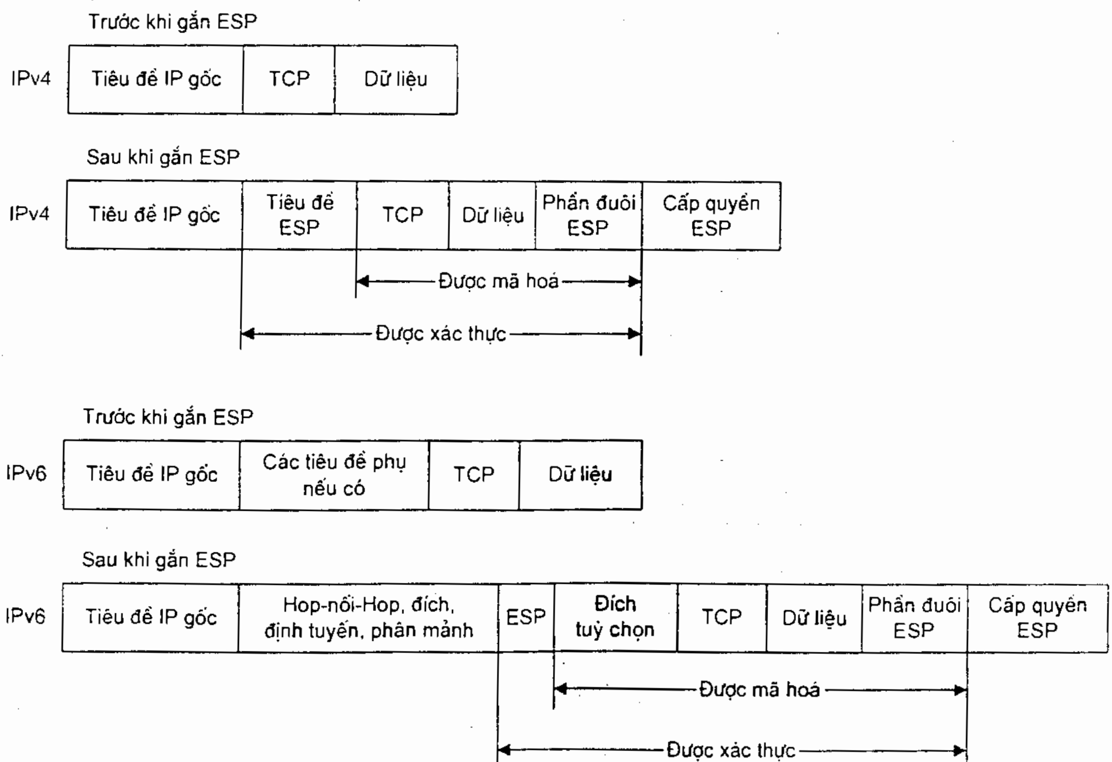
Khi nhận gói dữ liệu, đầu nhận sẽ tính toán giá trị bộ xác thực của riêng nó là 128 bit hay 160 bit (tuỳ theo là sử dụng loại nào), chia nhỏ nó ra tuỳ theo chiều dài được chỉ định trong trường xác thực và so sánh giá trị của nó với giá trị xác thực nhận được. Khi mà cả 2 giống nhau thì dữ liệu không bị thay đổi trên đường truyền. Do có thể có cuộc tấn công bằng cách chặn một loạt các gói và sau đó phát lại

chúng vào thời điểm sau nên AH cung cấp dịch vụ chống phát lại để ngăn chặn các tấn công dựa trên cách thức trên.

Cần chú ý là AH không giữ cho dữ liệu bí mật được. Nếu một kẻ tấn công chặn các gói trên mạng lại và sử dụng một mật mã thích hợp thì cũng có thể đọc được nội dung của dữ liệu mặc dù không thể thay đổi được nội dung của dữ liệu. Để bảo mật dữ liệu chống lại việc nghe trộm chúng ta cần phải sử dụng thành phần thứ 2 của IPSec đó là ESP.

5.1.3 Bọc gói bảo mật tải ESP

Bọc gói bảo mật tải ESP (Encapsulating Security Payload) được sử dụng cho việc mã hoá dữ liệu. Giống như tiêu đề AH, tiêu đề ESP được chèn vào giữa tiêu đề IP và nội dung tiếp theo của gói (hình 5.4). Tuy nhiên ESP có nhiệm vụ mã hoá dữ liệu nên nội dung của gói sẽ bị thay đổi.



Hình 5.4: Bọc gói bảo mật tải

Giống như tiêu đề AH, ESP gồm có SPI để chỉ cho bên nhận biết cơ chế bảo mật thích hợp cho việc xử lý gói. Số tuần tự trong tiêu đề ESP là bộ đếm sẽ tăng mỗi khi một gói được gửi đến cùng một địa chỉ và sử dụng cùng SPI. Số tuần tự chỉ ra có bao nhiêu gói được gửi có cùng một nhóm các tham số. Số tuần tự giúp cho

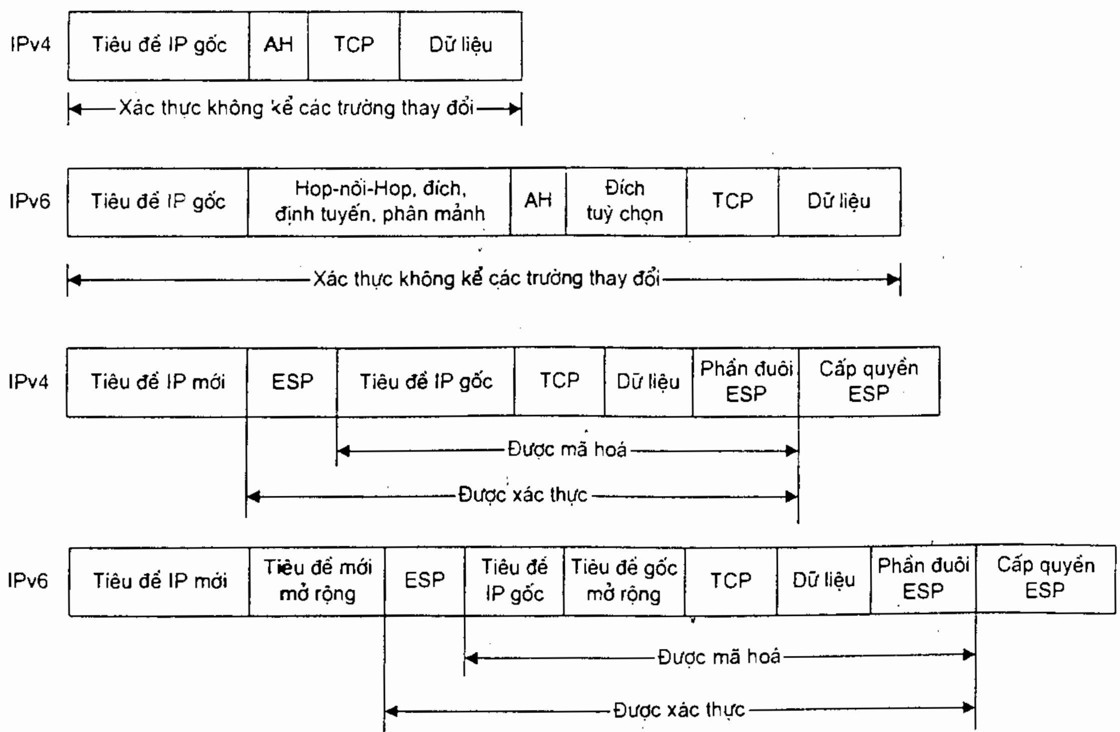
việc bảo mật chống lại các vụ tấn công bằng cách chép các gói và gửi chúng sai thứ tự để làm rối loạn quá trình truyền thông. Phần còn lại của gói (ngoại trừ xác thực dữ liệu) sẽ được mã hoá trước khi gửi lên mạng.

ESP có thể hỗ trợ bất kỳ giao thức mã hoá nào. Người dùng có thể dùng những giao thức khác nhau cho mỗi kết nối truyền thông. Tuy nhiên IPSec qui định mật mã DES-CBC (DES with Cipher Block Chaining) là giá trị mặc định để bảo đảm tính hoạt động liên mạng.

Sử dụng ESP yêu cầu khoá DES 56 bit. Để sử dụng một chuỗi các từ mã, một vector 64 bit được khởi động và dữ liệu được xử lý theo từng khối 64 bit.

ESP cũng có thể sử dụng cho mục đích xác thực. Trường xác thực ESP, một trường tuỳ chọn trong tiêu đề ESP, bao gồm một kiểm tra tổng mã hoá. Độ dài của tổng kiểm tra này thay đổi tuỳ theo giải thuật xác thực được sử dụng. Nó cũng có thể được bỏ qua nếu như dịch vụ xác thực không được chọn trong ESP. Xác thực được tính toán sau khi tiến trình mã hoá dữ liệu đã hoàn thành.

Dịch vụ xác thực cung cấp bởi AH khác so với ESP là dịch vụ xác thực trong ESP không bảo mật tiêu đề IP đặt trước ESP mặc dù nó bảo mật tiêu đề IP đã bọc gói trong chế độ đường hầm. Hình 5.5 minh hoạ sự khác biệt giữa chúng.



Hình 5.5 So sánh xác thực bởi AH và ESP

Nếu như AH được sử dụng với mục đích xác thực thì tại sao còn tuỳ chọn xác thực trong ESP? AH chỉ sử dụng trong những trường hợp khi xác thực gói là cần thiết. Mặt khác khi xác thực và tính riêng tư được yêu cầu thì sử dụng ESP với tuỳ chọn xác thực sẽ tốt hơn. Sử dụng ESP cho mã hoá và xác thực, thay vì sử dụng AH và ESP không có tuỳ chọn xác thực, sẽ giảm kích thước nên các gói sẽ được xử lý hiệu quả hơn.

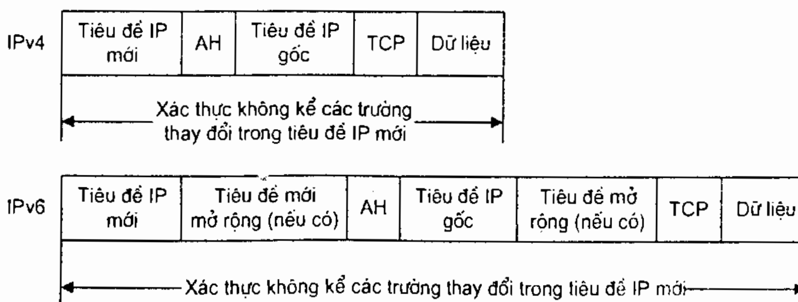
5.1.4 Chế độ làm việc

Có 2 chế độ làm việc trong IPSec:

- **Chế độ giao vận (Transport mode)**: chỉ có đoạn lớp giao vận trong gói là được xử lý.
- **Chế độ đường hầm (Tunnel mode)**: Toàn bộ gói sẽ được xử lý cho mã hoá xác thực.

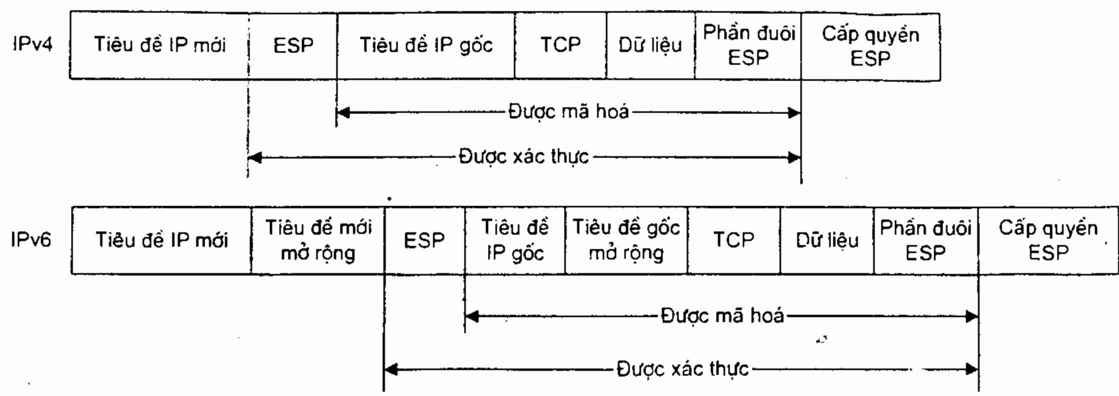
Chế độ giao vận sử dụng cho cả cổng nối và host, cung cấp cơ chế bảo mật cho các giao thức lớp trên. Trong chế độ giao vận, AH được chèn vào sau tiêu đề IP và trước các giao thức lớp trên (TCP, UDP hay ICMP) hoặc trước bất kỳ tiêu đề IPSec đã được chèn vào trước đó.

Trong chế độ đường hầm tiêu đề IP chứa địa chỉ nguồn và địa chỉ đích, trong khi bộ xuất tiêu đề IP chứa các địa chỉ IP khác (chẳng hạn như địa chỉ của cổng nối). AH bảo mật toàn bộ gói IP bao gồm cả bộ nhập tiêu đề IP (hình 5.6).

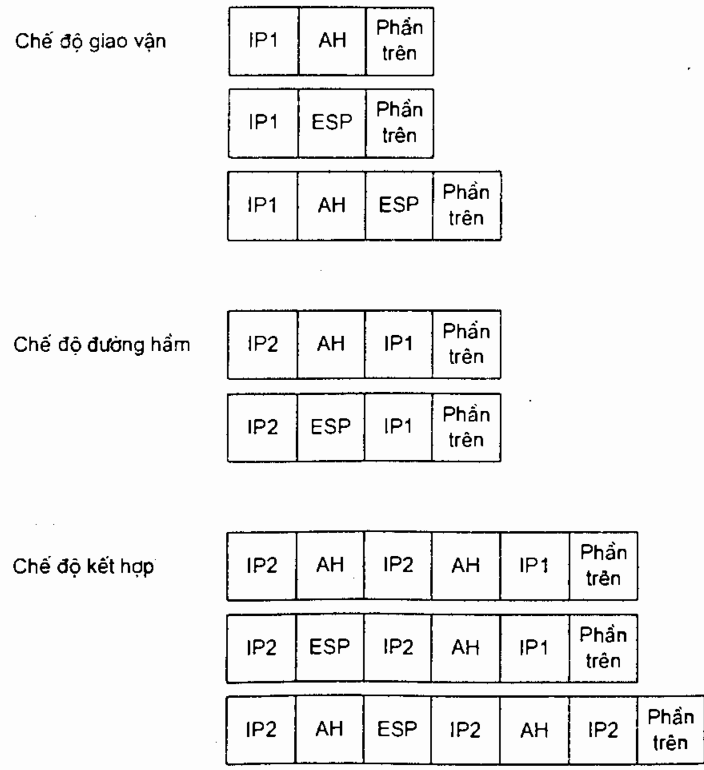


Hình 5.6: Chế độ đường hầm AH

Bởi vì AH chỉ bảo mật chống lại việc thay đổi nội dung dữ liệu nên cần phải có phương tiện khác để bảo đảm tính riêng tư của dữ liệu. Trong chế độ đường hầm điều đó được thực hiện bằng cách mở rộng bảo mật nội dung tiêu đề IP đặc biệt là địa chỉ nguồn và địa chỉ đích. Mặc dù trong chế độ giao vận ESP bảo mật chống lại nghe trộm một cách có hiệu quả nhưng nó không bảo mật được toàn bộ lưu lượng. Một vụ tấn công tinh vi vẫn có thể đọc được địa chỉ nguồn và địa chỉ đích sau đó sẽ phân tích lưu lượng để biết được phương thức truyền thông.



Hình 5.7: Chế độ đường hầm ESP



Hình 5.8: Các trường hợp của chế độ giao vận và đường hầm

Chế độ đường hầm ESP cung cấp thêm các cơ chế bảo mật cho các gói bằng cách mã hoá toàn bộ gói (hình 5.7).

Sau khi toàn bộ nội dung dữ liệu (bao gồm tiêu đề gốc) đã được mã hoá, chế độ đường hầm ESP sẽ tạo ra một tiêu đề IP mới để định tuyến cho các gói dữ liệu từ bên gửi đến bên nhận.

Thậm chí trong chế độ đường hầm, ESP cũng không bảo đảm chống lại được tất cả các loại phân tích lưu lượng vì địa chỉ IP của bên gửi và của cổng nối nhận vẫn có thể đọc được trong tiêu đề của gói. Điều này cho phép kẻ nghe trộm biết được có hai đối tượng đang truyền thông với nhau nhưng lại không có chút manh mối nào để biết hai đối tượng ấy là ai.

Để có thể áp dụng cả AH và ESP trong chế độ đường hầm hay chế độ giao vận, IPSec yêu cầu phải hỗ trợ được cho tổ hợp của chế độ đường hầm và chế độ giao vận (hình 5.8). Điều này được thực hiện bằng cách sử dụng chế độ đường hầm để mã hoá và xác thực các gói và tiêu đề của nó rồi gắn AH, ESP hoặc dùng cả hai trong chế độ giao vận để bảo mật cho tiêu đề mới được tạo ra.

Cần chú ý là AH và ESP không thể sử dụng chung trong chế độ đường hầm. Lý do là ESP đã có riêng tùy chọn xác thực, tuỳ chọn này nên sử dụng trong chế độ đường hầm khi các gói cần phải mã hoá và xác thực.

5.2 Quản lý khoá

Trong truyền thông sử dụng giao thức IPSec đòi hỏi phải có chuyển giao khoá do đó đòi hỏi phải có cơ chế quản lý khoá. Có hai phương thức để chuyển khoá đó là chuyển khoá bằng tay và chuyển khoá Internet IKE (Internet Key Exchange). Cả hai phương thức này không thể thiếu được trong IPSec. Một hệ thống IPSec phụ thuộc phải hỗ trợ phương thức chuyển khoá bằng tay. Phương thức chìa khoá trao tay này chẳng hạn như khoá thương mại ghi trên giấy, trên đĩa mềm hay thông qua gửi bưu phẩm hoặc e-mail. Mặc dù phương thức chìa khoá trao tay thích hợp với một số lượng nhỏ các site nhưng một phương thức quản lý tự động và kiểm soát được thì phù hợp với các yêu cầu tạo những SA. Giao thức quản lý chuyển giao khoá mặc định trong IPSec là Internet Key Exchange (IKE) là kết quả của kết hợp giữa bảo mật Internet ISA (Internet Security Association) và giao thức chuyển khoá (ISAKMP). IKE còn có một tên gọi khác là ISAKMP/Oakley.

IKE có các khả năng sau:

- Cung cấp các phương tiện cho 2 bên thoả thuận sử dụng các giao thức, giải thuật và khoá.
- Đảm bảo ngay từ lúc bắt đầu chuyển khoá là truyền thông đúng đối tượng.
- Quản lý các khoá sau khi chúng được chấp nhận trong tiến trình thoả thuận.
- Đảm bảo các khoá được chuyển một cách bảo mật.

Chuyển khoá tương tự như quản lý kết hợp (Internet Association). Khi cần tạo một SA cần phải chuyển khoá. Do đó cấu trúc của IKE bọc chúng lại với nhau và chuyển chúng đi như một gói tích hợp.

5.2.1 Các chế độ của Oakley và các pha của ISAKMP

Theo định nghĩa nguyên thủy trong ISAKMP thì IKE hoạt động 2 giai đoạn. Giai đoạn 1 thiết lập một đường hầm bảo mật cho các hoạt động ISAKMP diễn ra trên đó. Giai đoạn 2 là tiến trình đàm phán các mục đích SA.

Oakley đưa ra 3 chế độ chuyển khoá và cài đặt các ISAKMP SA: hai cho giai đoạn 1 của ISAKMP và một cho giai đoạn 2.

- Chế độ chính (Main mode): Hoàn thành giai đoạn 1 của ISAKMP sau khi đã thiết lập một kênh bảo mật.
- Chế độ năng động (Aggressive mode): Một cách khác để hoàn thành giai đoạn một của ISAKMP. Nó đơn giản hơn và nhanh hơn chế độ chính, nhưng không bảo mật nhận dạng cho việc đàm phán giữa các nút, bởi vì nó truyền nhận dạng của chúng trước khi đàm phán được một kênh bảo mật.
- Chế độ nhanh (Quick mode): Hoàn thành giai đoạn 2 của ISAKMP bằng cách đàm phán một SA cho các mục đích của việc truyền thông.

IKE cũng còn một chế độ khác đó là chế độ nhóm mới, chế độ này không thật sự là của giai đoạn 1 hay giai đoạn 2. Chế độ nhóm mới theo sau đàm phán của giai đoạn và đưa ra một cơ chế định nghĩa nhóm riêng cho chuyển giao Diffie-Hellman.

Để thiết lập một bảo mật IKE cho một nút, một host hay một cổng nối cần ít nhất 4 yếu tố:

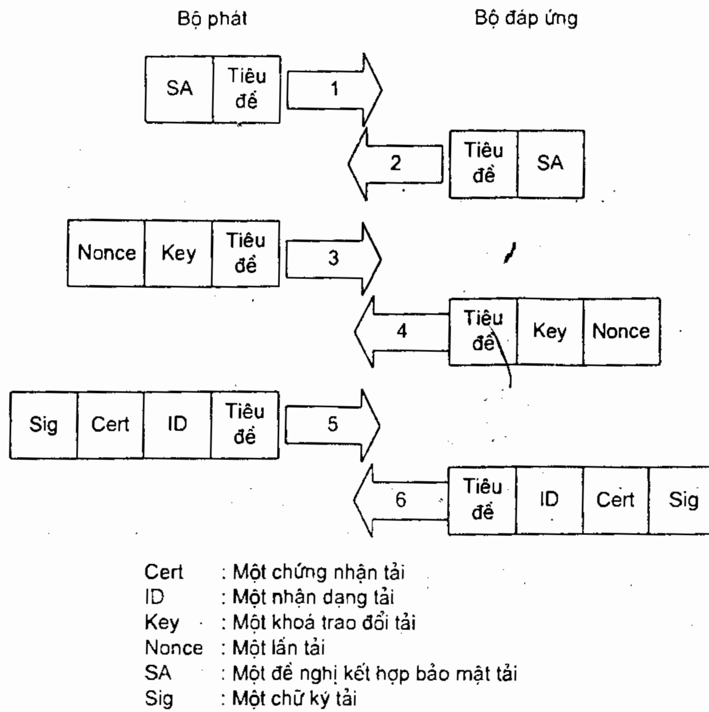
- Một giải thuật mã hoá để bảo mật dữ liệu.
- Một giải thuật băm để giảm dữ liệu cho báo hiệu.
- Một phương thức xác thực cho báo hiệu dữ liệu.
- Thông tin về nhóm làm việc qua tổng đài.

Yếu tố thứ 5 có thể được đưa ra trong SA, hàm giả ngẫu nhiên (pseudo-random function) sử dụng để băm giá trị hiện tại xuống quá trình chuyển khoá cho mục đích kiểm tra. Nếu trong SA không bao gồm nó thì HMAC của giải thuật băm (yếu tố thứ 2) được sử dụng.

Chế độ chính

Chế độ chính đưa ra cơ chế để thiết lập giai đoạn một của ISAKMP SA, bao gồm các bước sau:

- Sử dụng chế độ chính để khởi động một ISAKMP SA cho kết nối tạm.
- Sử dụng chế độ nhanh để đàm phán một SA.
- Sử dụng SA được tạo ra ở trên để truyền thông cho đến khi nó hết hạn.



Hình 5.10: Chế độ chính ISAKMP

Bước thứ nhất, sử dụng chế độ chính để bảo mật một ISAKMP SA, diễn ra theo 3 bước trao đổi hai chiều giữa SA gửi và SA nhận (hình 5.10). Bước trao đổi đầu tiên thoả thuận về giải thuật và băm. Bước trao đổi thứ 2 chuyển giao khoá chung và các nonce của nhau (là những con số ngẫu nhiên mà một bên ghi và trả lại để chứng minh danh định của nó). Bước thứ 3, hai bên sẽ kiểm tra danh định của nhau và tiến trình trao đổi hoàn tất.

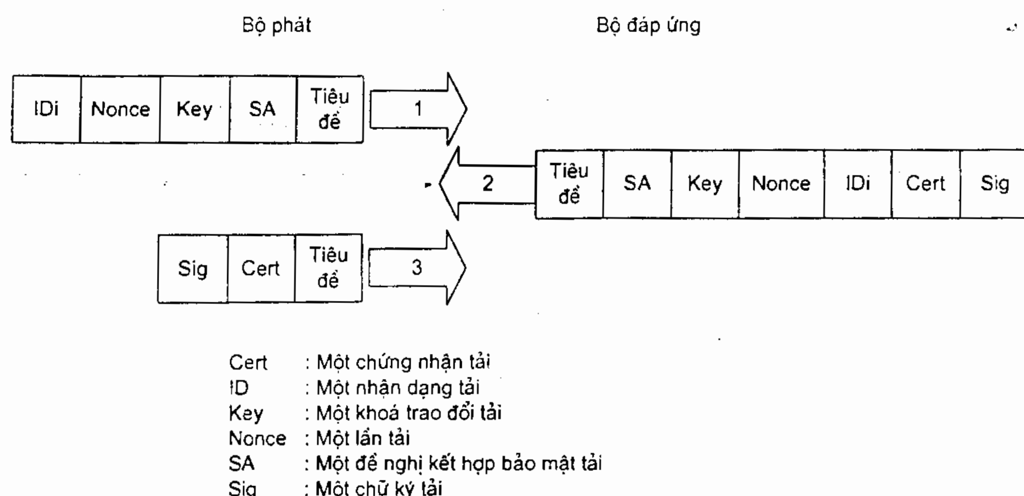
Hai bên có thể sử dụng khoá dùng chung khi chúng nhận được. Hai bên phải băm chúng 3 lần: đầu tiên tạo ra một khoá gốc (để sử dụng tạo khoá phụ trong chế độ nhanh sau này), sau đó là khoá xác thực và cuối cùng khoá mã để sử dụng cho ISAKMP SA.

Chế độ chính bảo mật các danh định của các đối tượng truyền thông. Nếu như không cần việc bảo mật, để cho việc trao đổi nhanh hơn, thì chế độ năng động được sử dụng.

Chế độ năng động

Chế độ năng động (Aggressive mode) đưa ra dịch vụ cũng tương tự như chế độ chính là thiết lập một ISAKMP SA nguyên thủy. Chế độ năng động trông cũng giống như chế độ chính ngoại trừ chỉ có 2 bước trao đổi thay vì 3 bước như chế độ chính.

Trong chế độ năng động khi bắt đầu chuyển đổi bên phát sẽ tạo ra một đôi Diffie-Hellman, đưa ra một SA, chuyển đi giá trị Diffie-Hellman công cộng, gửi một nonce cho đầu bên kia ghi nhận và gửi một gói ID để bên đáp ứng có thể sử dụng để kiểm tra danh định. Phía đáp ứng có thể gửi trả về mọi thứ cần thiết để hoàn tất quá trình chuyển đổi. Việc đáp ứng này tổ hợp 3 bước đáp ứng trong chế độ chính thành một do đó bên khởi đầu chỉ cần xác thực việc chuyển đổi (hình 5.11).



Hình 5.11: Chế độ năng động ISAKMP

Do chế độ năng động không đưa ra cách bảo mật danh định cho các bên tham gia truyền thông nên cần phải trao đổi thông tin danh định trước khi thiết lập một SA bảo mật. Ai đó theo dõi việc chuyển đổi theo chế độ năng động có thể nhận diện ai đã thiết lập một SA mới. Ưu điểm của chế độ năng động là tốc độ.

Chế độ nhanh

Sau khi hai đối tượng đã thiết lập một ISAKMP SA bằng chế độ chính hay chế độ năng động thì tiếp đến là sử dụng chế độ nhanh (Quick Mode).

Chế độ nhanh có hai mục đích là: đàm phán về dịch vụ bảo mật IPSec và tạo ra vật liệu khoá tươi (fresh keying material). Chế độ nhanh được coi là đơn giản hơn chế độ chính và chế độ năng động. Bởi vì nó đã có sẵn một đường hầm bên trong (tất cả các gói đều được mã hoá). Các gói chế độ nhanh đều được mã hoá và được khởi tạo với một tải băm. Tải băm được tạo ra bằng cách dùng một hàm tạo giả ngẫu nhiên đã được đồng ý trước và một khoá xác thực nhận được. Tải băm dùng để xác thực phần còn lại của gói dữ liệu. Chế độ nhanh định nghĩa những phần nào của gói dữ liệu nằm trong phần băm.

Khoá có thể được làm tươi bằng 1 hay 2 cách: Nếu như không cần chuyển tiếp một cách bí mật hoàn toàn thì chế độ nhanh chỉ làm tươi khoá trong chế độ chính hay chế độ năng động với băm thêm. Hai đối tượng truyền thông có thể gửi các nonce qua đường hầm bảo mật và dùng chúng để băm khoá đang tồn tại. Nếu như cần chuyển tiếp một cách bí mật hoàn toàn thì có thể yêu cầu thêm một chuyển đổi Diffie-Hellman thông qua SA đang tồn tại và đổi giá trị của khoá.

Bộ phát
Bộ đáp ứng
ID/ID | {Key} | Nonce | SA | Hash 1 | Tiêu đề → 1
2 ← Tiêu đề | Hash 2 | SA | Nonce | {Key}
Hash 3 | Tiêu đề → 3

Cert : Một chứng nhận tải
ID : Một nhận dạng tải
Key : Một khoá trao đổi tải
Nonce : Một lần tải
SA : Một đề nghị kết hợp bảo mật tải
Hash : Một tải băm
{} : Chỉ thị một tuỳ chọn tải

Hình 5.12 Chế độ nhanh ISAKMP

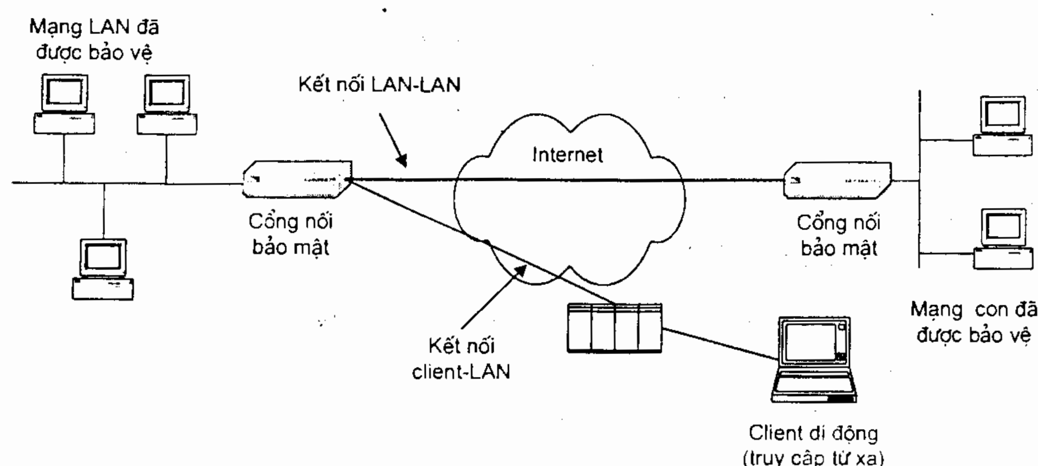
5.2.2 Đàm phán SA

Để thiết lập một SA bên khởi tạo gửi một thông báo chế độ nhanh thông qua yêu cầu một SA mới của ISAKMP SA. Một đàm phán SA là kết quả của hai SA: một hướng về (inbound) đến bên khởi tạo và một hướng đi (outbound). Để tránh xung đột về SPI, nút nhận phải luôn chọn SPI. Do đó trong chế độ nhanh bên phát thông báo cho bên đáp ứng biết SPI sẽ sử dụng và bên đáp ứng sẽ theo SPI đã được chọn. Mỗi SPI, kết hợp với địa chỉ IP đích, chỉ định một IPSec SA đơn duy nhất. Tuy nhiên trên thực tế những SA này luôn có hai hướng về và đi, chúng có danh định về tham số, giải thuật, khoá, băm là một phần trong SPI.

5.3 Sử dụng IPSec

Hình 5.13 là một ví dụ về ứng dụng Internet VPN. Có 3 nơi trang bị phần mềm IPSec là: cổng nối bảo mật, client di động (mobile client) và các host. Tuy nhiên, không phải tất cả các thiết bị đều cần phải cài phần mềm IPSec mà tuỳ theo yêu cầu thiết kế mạng. Ví dụ cần tạo kết nối LAN-LAN VPN thì cổng nối bảo mật IPSec là đủ. Nếu cần cho các trạm làm việc từ xa quay số truy cập vào mạng thông

qua các ISP (Internet Service Provider) thì phần mềm client IPSec cần cài trên các máy tính của các đối tượng di động. Nếu muốn tạo một VPN mà tất cả các máy tính có thể liên lạc với các máy tính thông qua giao thức IPSec thì cần phải cài đặt phần mềm IPSec trên tất cả các máy tính.



Hình 5.13: Các thành phần của một Internet VPN

5.3.1 Các cổng nối bảo mật

Cổng nối bảo mật (security gateway) là một thiết bị mạng chẳng hạn như bộ định tuyến hay tường lửa, chia cắt và bảo mật mạng bên trong chống lại xâm nhập không được cho phép từ bên ngoài. Sử dụng IPSec trên cổng nối bảo mật làm cho lưu lượng qua cổng nối bảo mật bị thắt nút cổ chai trước khi ra bên ngoài.

Khi xây dựng một VPN thì cần cài cổng nối bảo mật tại các văn phòng chính và sau đó thiết lập liên kết bảo mật giữa các cổng nối bảo mật với nhau. Sử dụng cổng nối bảo mật làm giảm độ phức tạp của việc quản lý các khoá vì chỉ cần gán một khoá duy nhất cho cổng nối bảo mật. Cổng nối bảo mật có thể chuyển các gói dù là ở chế độ giao vận hay chế độ đường hầm. Để cho độ bảo mật cao thì chế độ đường hầm thích hợp hơn do nó giấu đi các địa chỉ IP thật sự của người gửi và người nhận và bảo mật chống lại các tấn công cắt-dán tiêu đề (header cut-and-paste). Tuy nhiên chế độ đường hầm đòi hỏi phải có tính toán ở cổng nối bảo mật và làm tăng kích thước gói nên sẽ làm giảm thông lượng của mạng. Sử dụng chế độ giao vận giữa các cổng nối sẽ làm giảm tổng phí truyền thông nhưng nó không giấu các địa chỉ IP thực của nguồn và đích. Nếu như bảo mật đại diện (wild card) không được sử dụng cho lưu lượng qua cổng nối bảo mật thì cơ chế quản lý khoá sẽ thêm phức tạp hơn.

5.3.2 Các SA đại diện

Bảo mật đại diện (wild card) làm cho việc truyền thông giữa các host được bảo mật bởi cổng nối bảo mật trở nên đơn giản hơn. Thay vì kết hợp một SA với một địa chỉ IP host duy nhất thì bảo mật đại diện kết hợp tất cả các host trên LAN được phục vụ bởi cổng nối bảo mật.

Sau đây là một số đặc tính và khả năng mà một cổng nối bảo mật phải có:

- Hỗ trợ các kết nối mạng cho văn bản đơn giản hoặc văn bản đã được mã hoá.
- Chiều dài của từ khoá phải không phụ thuộc vào mật độ thông tin truyền trên lớp liên kết dữ liệu.
- Phải hỗ trợ cả AH và ESP.
- Hỗ trợ tạo SA bằng tay, bao gồm cả bảo mật đại diện.
- Có cơ chế bảo mật khoá.
- Hệ thống thay đổi khoá một cách tự động và hệ thống quản lý khoá phải đơn giản nhưng bảo mật.
- SA phải có các thông báo về lỗi.

5.3.3 Host từ xa

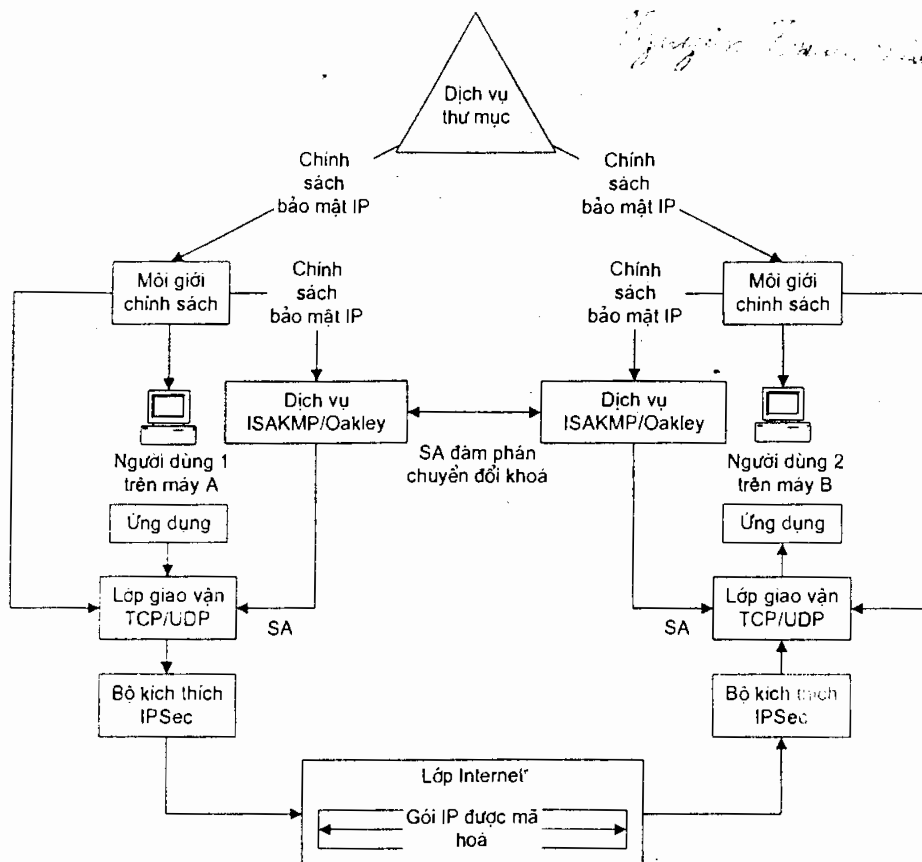
Khi dùng một máy tính quay số kết nối vào mạng VPN cần phải có một phần mềm client IPSec cài trên đó. Với IPv4 thì IPSec được chèn trong chồng giao thức TCP/IP. Mã IPSec có thể được chèn vào giữa lớp giao vận và lớp mạng. IPSec cũng có thể được chèn vào như miếng chêm giữa lớp liên kết dữ liệu và lớp mạng.

Cách đầu rất mềm dẻo đối với người dùng vì nó cho phép họ gán những SA khác nhau cho các phần mềm khác nhau hay nói một cách khác một số lưu lượng có thể truyền đi mà không có IPSec do nó không cần thiết, phần lưu lượng quan trọng còn lại truyền đi với bảo mật của IPSec. Miếng chêm (shim) có thể tiếp cận một cách dễ dàng hơn nhưng nó chỉ có hiệu lực bảo mật ở mức địa chỉ IP còn không hiệu lực ở mức nhận dạng người dùng.

Các yêu cầu đối với một phần mềm client IPSec:

- Tương thích với các công cụ IPSec khác (chẳng hạn như thích hợp với máy chủ mã hoá của các site).
- Đưa ra một chỉ báo rõ ràng khi IPSec đang hoạt động.
- Hỗ trợ tải SA về.
- Hàm băm xử lý được các địa chỉ IP động.
- Có cơ chế bảo mật khoá chống lại kẻ trộm (mã hoá khoá với mật khẩu).

- Có cơ chế chuyển đổi mã một cách tự động và định kỳ.
- Chặn hoàn toàn các lưu lượng không-IPSec.



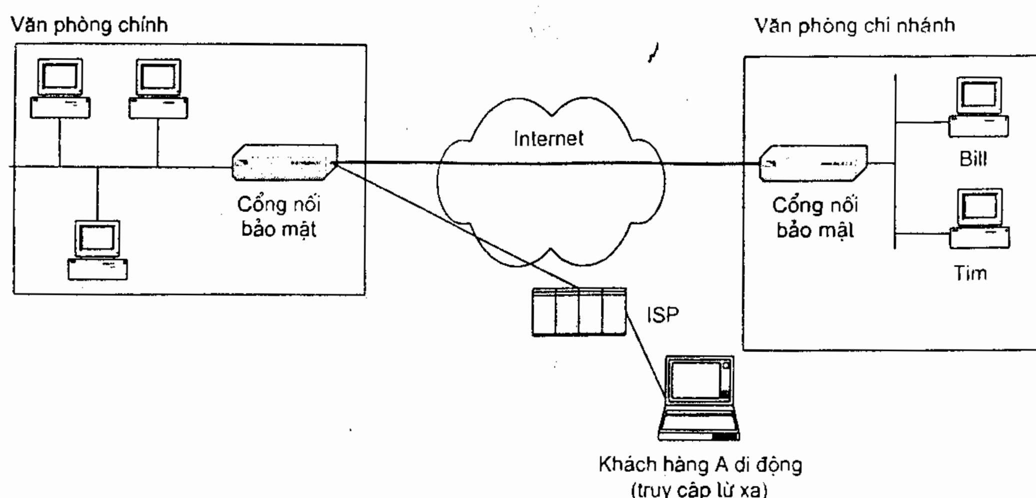
Hình 5.14: IPSec và các chính sách bảo mật

5.3.4 Một ví dụ minh hoạ

Để minh họa việc sử dụng IPSec để xây dựng VPN, hãy xem xét một thiết kế đơn giản trong hình 5.15 gồm 2 site: một ở văn phòng chính và một ở văn phòng chi nhánh. Mạng cũng cung cấp khả năng cho các người dùng di động có thể quay số truy cập vào VPN thông qua các ISP địa phương. Sử dụng bộ định tuyến mã hoá để làm cổng nối bảo mật. Lượng truyền bên trong mạng dưới dạng văn bản đơn giản và dùng kỹ thuật bảo mật chống lại sự tấn công từ bên ngoài là tường lửa hay danh sách điều khiển truy cập trên máy chủ. Chỉ có lưu lượng giữa các site hay giữa các người dùng di động và các site là được bảo mật bởi IPSec.

Để bảo mật cho hệ thống, cần phải có cơ chế bảo mật vật lý để đảm bảo tất cả các host trong phạm vi site có đúng các tham số vật lý và mọi ngõ ra bên ngoài

đều phải đi qua bộ định tuyến mã hoá. Tất cả các kết nối từ các site bên trong mạng và các site ngoài mạng cần phải được khoá lại với đặc quyền truy cập. Nếu như số lượng site trong mạng tăng lên thì cần phải có một trung tâm làm nhiệm vụ gán các SA và khoá



Hình 5.15: Ví dụ về IPSec VPN

5.4 Các vấn đề còn tồn đọng trong IPSec

Mặc dù IPSec đã sẵn sàng đưa ra các đặc tính cần thiết cho việc bảo mật một VPN thông qua Internet nhưng nó vẫn còn trong giai đoạn phát triển. Tất cả các gói được xử lý theo IPSec sẽ làm tăng kích thước do thêm vào các tiêu đề IPSec làm cho thông lượng của mạng giảm xuống. Điều này có thể được giải quyết bằng cách nén nội dung dữ liệu trước khi mã hoá, nhưng điều này chưa được chuẩn hoá.

IKE vẫn là công nghệ chưa được chứng minh. Phương thức chuyển khoá bằng tay lại không thích hợp cho mạng có một số lượng lớn các đối tượng di động.

IPSec được thiết kế chỉ để điều khiển lưu lượng IP mà thôi.

Việc tính toán cho nhiều giải thuật trong IPSec vẫn còn là một vấn đề đối với các trạm làm việc và máy PC cũ.

Việc phân phối các phần cứng và phần mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số nước.

Sử dụng IPSec ở chế độ đường hầm cho phép các nút có thể có những địa chỉ IP không hợp lệ nhưng vẫn có thể liên lạc được với các nút khác. Nhưng khi chuyển xuống bảo mật mức host thì các địa chỉ IP đó phải được quản lý cẩn thận sao cho nhận dạng được nhau.

CHƯƠNG 6

GIAO THỨC PPTP

Giao thức định đường hầm điểm-điểm PPTP (Point-to-Point Tunneling Protocol) được đưa ra đầu tiên bởi một nhóm các công ty được gọi là PPTP forum. Nhóm này bao gồm 3Com, Ascend comm, Microsoft, ECI Telematicsunication và US Robotic. Ý tưởng cơ sở cho giao thức này là tách các chức năng chung và riêng của truy cập từ xa, lợi dụng lợi ích của cơ sở hạ tầng Internet sẵn có để tạo kết nối bảo mật giữa client và mạng riêng. Người dùng xa chỉ việc quay số tới nhà cung cấp dịch vụ Internet địa phương là có thể tạo một đường hầm bảo mật tới mạng riêng của họ.

Giao thức quay số truy cập vào Internet phổ biến nhất là giao thức điểm-điểm PPP (Poit-to-Point Protocol). PPTP được xây dựng dựa trên chức năng của PPP, cung cấp khả năng quay số truy cập tạo ra một đường hầm bảo mật thông qua Internet đến site đích. PPTP sử dụng giao thức bọc gói định tuyến chung GRE (Generic Routing Encapsulation) được mô tả lại để đóng và tách gói PPP (hình 6.1), giao thức này cho phép PPTP mềm dẻo xử lý các giao thức khác không phải là IP như IPX, NETBEUI chẳng hạn.

Bởi vì PPTP dựa trên PPP nên nó dựa vào cơ chế xác thực của PPP có tên là PAP và CHAP. PPTP có thể sử dụng PPP để mã hoá dữ liệu nhưng Microsoft đã đưa ra một phương thức mã hoá khác mạnh hơn đó là mã hoá điểm-điểm MPPE (Microsoft Point-to-Point Encryption) để sử dụng cho PPTP.

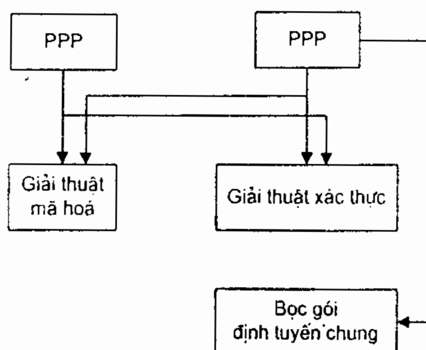
Một ưu điểm của PPTP là được thiết kế để hoạt động ở lớp thứ 2 (lớp liên kết dữ liệu) trong khi IPSec chạy ở lớp thứ 3. Bằng cách hỗ trợ việc truyền dữ liệu ở lớp thứ 2, PPTP có thể truyền trong đường hầm bằng các giao thức khác IP trong khi IPSec chỉ có thể truyền các gói IP trong đường hầm.

6.1 Dạng thức của PPTP

6.1.1 PPP và PPTP

PPP đã trở thành giao thức quay số truy cập vào Internet và các mạng TCP/IP rất phổ biến hiện nay. Làm việc ở lớp thứ 2 trong mô hình OSI (lớp liên kết dữ liệu) PPP bao gồm các phương thức đóng tách gói cho các loại gói dữ liệu khác nhau để truyền nối tiếp. PPP đặc biệt định nghĩa 2 bộ giao thức: giao thức điều khiển liên kết LCP (Link Control Protocol) cho việc thiết lập, cấu hình và kiểm tra kết nối; một loạt các giao thức điều khiển mạng NCP (Network Control Protocols) cho việc thiết lập và cấu hình các giao thức lớp mạng khác nhau.

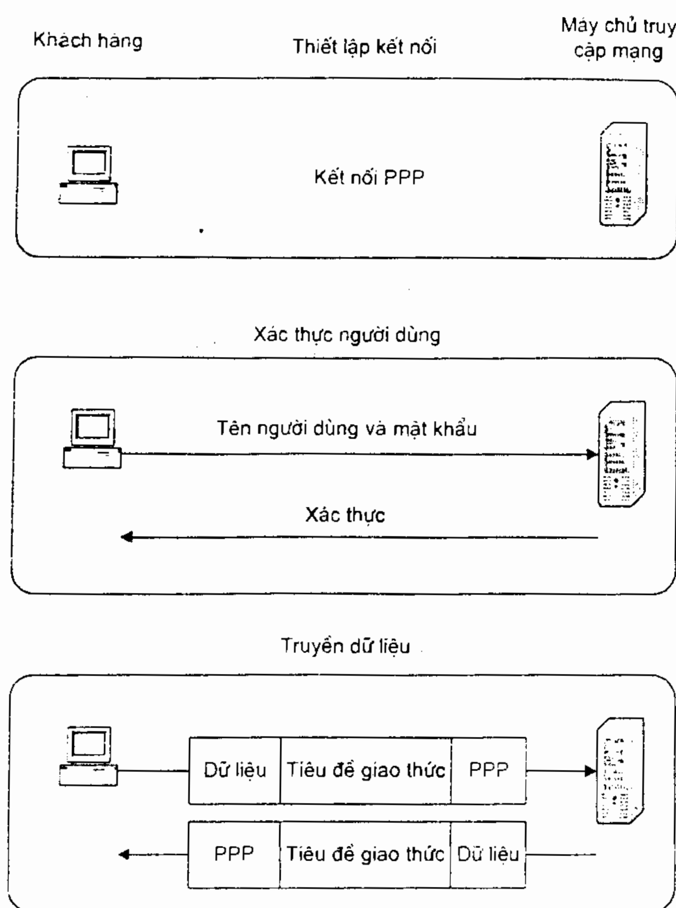
PPP đóng gói các gói IP, IPX, NETBEUI và truyền đi trên kết nối điểm-điểm từ máy gửi đến máy nhận (hình 6.2). Để việc truyền thông có thể diễn ra được mỗi PPP phải gửi gói LCP để cấu hình và kiểm tra liên kết dữ liệu.



Hình 6.1: Kiến trúc của PPTP

Khi một kết nối PPP được thiết lập thì người dùng thường đã được xác thực. Đây là giai đoạn tuỳ chọn trong PPP, tuy nhiên nó luôn luôn được cung cấp bởi các ISP và là một phần trong VPN. Việc xác thực phải diễn ra trước pha lớp mạng. Trong giao thức PPP, quá trình xác thực được tiến hành thông qua bởi PAP hay CHAP.

Với PAP mật khẩu được gửi qua kết nối dưới dạng văn bản đơn giản và không có bảo mật nào để tránh khỏi bị tấn công thử và lỗi. CHAP là một phương thức xác thực mạnh hơn, sử dụng phương thức bắt tay 3 chiều. CHAP chống lại các vụ tấn công quay lại bằng cách sử dụng các giá trị thách đố (challenge value) duy nhất và không thể đoán trước được. Vì CHAP phát ra giá trị thách đố trong suốt và sau khi thiết lập xong kết nối, lặp lại các thách đố có thể giới hạn số lần bị đặt vào tình thế bị tấn công.



Hình 6.2: Quay số mạng dùng PPP

PPTP dựa trên PPP để tạo ra kết nối quay số giữa khách hàng và máy chủ truy cập mạng. PPTP sử dụng PPP để thực thi các chức năng:

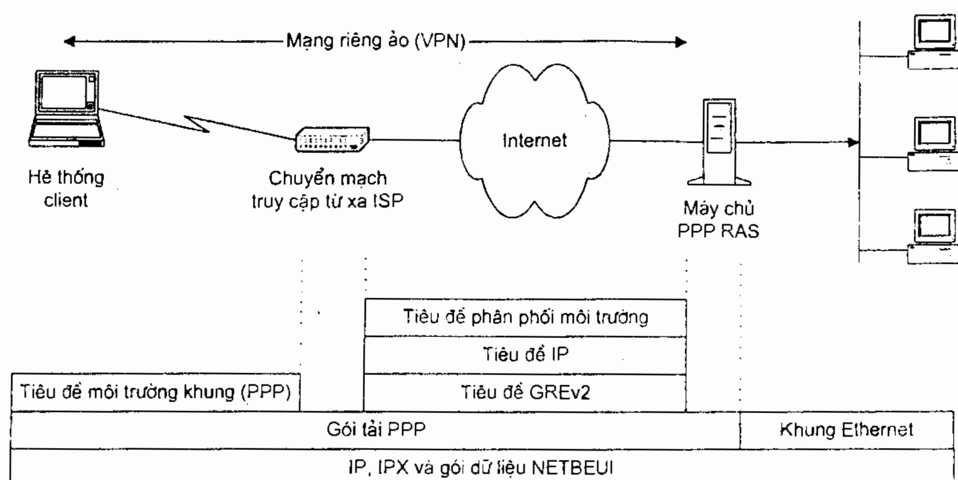
- Thiết lập và kết thúc kết nối vật lý.
- Xác thực các người dùng.
- Tạo ra gói dữ liệu PPP.

Sau khi PPP thiết lập kết nối, PPTP sử dụng các quy luật đóng gói của PPP để đóng gói các gói truyền trong đường hầm (hình 6.3).

Để tận dụng ưu điểm của kết nối tạo ra bởi PPP, PPTP định nghĩa 2 loại gói: gói điều khiển và gói dữ liệu và gán chúng vào 2 kênh riêng. Sau đó PPTP phân tách các kênh điều khiển và kênh dữ liệu thành luồng điều khiển với giao thức TCP và luồng giữ liệu với giao thức IP. Kết nối TCP được tạo giữa client PPTP và máy chủ PPTP được sử dụng để chuyển thông báo điều khiển.

Các gói dữ liệu là dữ liệu thông thường của người dùng. Các gói điều khiển được gửi đi theo chu kỳ để lấy thông tin về trạng thái kết nối và quản lý báo hiệu giữa client PTP và máy chủ mạng. Các gói điều khiển cũng được dùng để gửi các thông tin quản lý thiết bị, thông tin cấu hình giữa 2 đầu đường hầm.

Kênh điều khiển được yêu cầu cho việc thiết lập một đường hầm giữa client PTP và máy chủ PPTP. Phần mềm client có thể nằm ở máy người dùng từ xa hay nằm ở tại máy chủ của ISP.

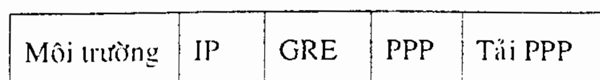


Hình 6.3 Các giao thức được dùng trong một kết nối PPTP

Sau khi đường hầm được thiết lập thì dữ liệu người dùng được truyền từ client đến máy chủ PPTP. Các gói PPTP chứa các gói dữ liệu IP. Gói dữ liệu IP được đóng gói bởi tiêu đề GRE (hình 6.4), sử dụng số ID của host cho điều khiển truy cập, ACK cho giám sát tốc độ dữ liệu truyền trong đường hầm.

Bởi vì PPTP hoạt động ở lớp liên kết dữ liệu, nên cần phải có tiêu đề môi trường truyền trong gói để cho biết dữ liệu truyền trong đường hầm theo phương thức nào. Tùy theo kiến trúc hạ tầng của các nhà ISP mà các phương thức này có thể là Ethernet, Frame Relay hay kết nối PPP.

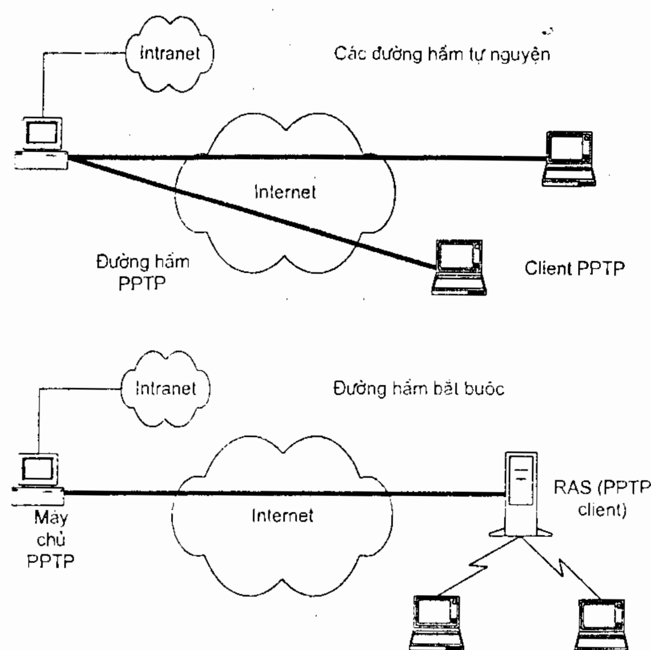
PPTP cũng có cơ chế điều khiển tốc độ nhằm giới hạn số lượng dữ liệu truyền đi. Cơ chế này làm giảm tối thiểu kích thước dữ liệu phải truyền lại do mất gói.



Hình 6.4: Bọc gói PPTP/GRE

6.1.2 Đường hầm

PPTP cho phép người dùng và các ISP có thể tạo ra nhiều loại đường hầm khác nhau. Người dùng có thể chỉ định điểm kết thúc của đường hầm ở ngay tại máy tính của mình nếu như có cài client PTP, hay tại máy chủ của ISP nếu như máy tính của họ chỉ có PPP mà không có PPTP. Đối với trường hợp thứ 2 thì máy chủ của ISP phải có hỗ trợ PPTP. Việc phân chia như vậy là kết quả của việc chia đường hầm thành 2 lớp: tự nguyện và bắt buộc (hình 6.5).



Hình 6.5: Các đường hầm tự nguyện và bắt buộc

Đường hầm tự nguyện được tạo ra theo yêu cầu của người dùng cho mục đích xác định. Khi sử dụng đường hầm tự nguyện, người dùng có thể đồng thời mở một đường hầm bảo mật thông qua Internet và có thể truy cập đến một host trên Internet bằng giao thức TCP/IP bình thường. Đường hầm tự nguyện thường được sử dụng để cung cấp tính riêng tư và toàn vẹn dữ liệu cho lưu lượng Intranet được gửi thông qua Internet.

Do đường hầm bắt buộc được tạo ra không thông qua người dùng nên nó trong suốt đối với người dùng đầu cuối. Điểm kết thúc của đường hầm bắt buộc nằm ở máy chủ truy cập từ xa. Tất cả dữ liệu truyền đi từ người dùng qua đường hầm PPTP thông qua RAS.

Bởi vì đường hầm bắt buộc định trước điểm kết thúc và người dùng không thể truy cập phần còn lại của Internet nên nó điều khiển truy cập tốt hơn là đường hầm tự nguyện. Nếu như vì tính bảo mật mà không cho người dùng truy cập

Internet công cộng thì đường hầm bắt buộc ngăn không cho họ truy cập Internet công cộng nhưng vẫn cho phép dùng Internet để truy cập VPN (nghĩa là chỉ truy cập vào được các site trong VPN mà thôi).

Một ưu điểm nữa của đường hầm bắt buộc là một đường hầm có thể tải nhiều kết nối. Đặc tính này làm giảm yêu cầu băng thông mạng cho các ứng dụng đa phiên làm việc.

Một khuyết điểm của đường hầm bắt buộc là kết nối từ RAS đến người dùng nằm ngoài đường hầm nên dễ bị tấn công.

Một đường hầm bắt buộc tĩnh được cấu hình bởi thiết bị hay bằng tay. Cấu hình bằng thiết bị yêu cầu người dùng gọi một số điện thoại đặc biệt để tạo kết nối. Cấu hình bằng tay, RAS sẽ kiểm tra một phần của tên người dùng gọi là realm, để quyết định nơi nào sẽ liên lạc với người dùng đó.

Có một cách tiếp cận mềm dẻo hơn đó là chọn đường hầm đích động khi người dùng kết nối với RAS. Những đường hầm động này được thiết lập trong PPTP bằng cách kết nối hệ thống với máy chủ RADIUS.

Đường hầm tĩnh đòi hỏi phải có một máy chủ truy cập mạng NAS (Network Access Server). Đứng về góc độ nhà cung cấp dịch vụ Internet ISP thì yêu cầu này không được mong muốn vì nó đòi hỏi ISP phải cung cấp một NAS cho khách hàng thay vì có thể dùng chung NAS đã có sẵn. Dó đó đường hầm tĩnh rất tốn tiền cho dịch vụ toàn cầu.

Đường hầm Realm cơ bản cho phép người dùng với một realm cho trước được đối xử như nhau, tuy nhiên nó giới hạn tính mềm dẻo của việc quản lý quyền truy cập của người dùng.Ví dụ như một công ty A cung cấp cho Jim một account vừa có thể truy cập Internet và Intranet, trong đó quyền truy cập Intranet được cung cấp bởi máy chủ đường hầm ở văn phòng B. Công ty A lại cung cấp cho Sam một account chỉ cho phép truy cập Intranet, account này được cung cấp bởi máy chủ đường hầm ở văn phòng C. Những tình huống như vậy đường hầm realm không thể dàn xếp được.

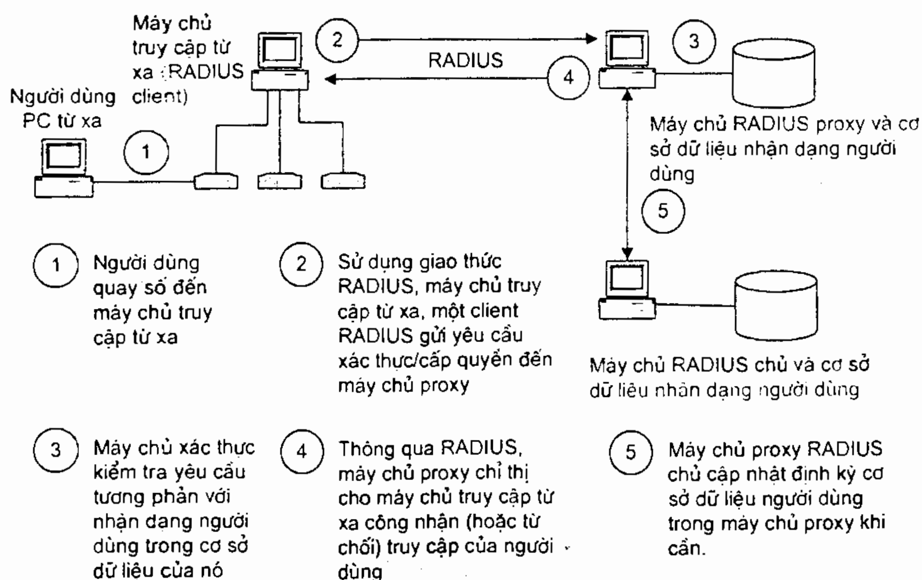
Sử dụng RADIUS để cung cấp đường hầm bắt buộc có một vài ưu điểm. Các đường hầm có thể được định nghĩa và kiểm tra dựa trên xác thực người dùng và tính cước có thể dựa trên số điện thoại, hoặc các phương thức xác thực khác, chẳng hạn như thẻ bài (token) hay thẻ thông minh (smart card).

6.1.3 RADIUS

RADIUS client/server sử dụng máy chủ truy cập mạng NAS (Network Access Server) để quản lý kết nối người dùng. Mặc dù các chức năng của NAS tương tự như chức năng của một máy chủ truy cập mạng nhưng nó cũng có một số

chức năng cho RADIUS client. NAS sẽ nhận lấy nhận dạng người dùng, thông tin về mật khẩu rồi chuyển thông tin bảo mật đến máy chủ RADIUS. Máy chủ RADIUS sẽ trả lại trạng thái xác thực là chấp nhận hay từ chối dữ liệu cấu hình cho NAS để cung cấp dịch vụ cho người dùng. RADIUS tạo một cơ sở dữ liệu tập trung về các người dùng, các loại dịch vụ sẵn có, một dải modem đa chủng loại. Trong RADIUS thông tin người dùng được lưu trữ tại máy chủ RADIUS. Bởi vì tất cả các thiết bị có hỗ trợ RADIUS đều có thể trở thành RADIUS client nên người dùng có thể được phép truy cập với cùng loại dịch vụ tại bất kỳ máy chủ nào có nối kết với máy chủ RADIUS.

RADIUS hỗ trợ cho máy chủ proxy, nơi lưu trữ thông tin người dùng cho mục đích xác thực và dùng để tính cước, cấp quyền, nhưng nó không cho phép dữ liệu người dùng (mật khẩu,..) được phép thay đổi. Một máy chủ proxy sẽ định kì cập nhật cơ sở dữ liệu người dùng từ máy chủ RADIUS chính (hình 6.6).



Hình 6.6: Tác động qua lại giữa một máy chủ RADIUS, máy chủ proxy và các client

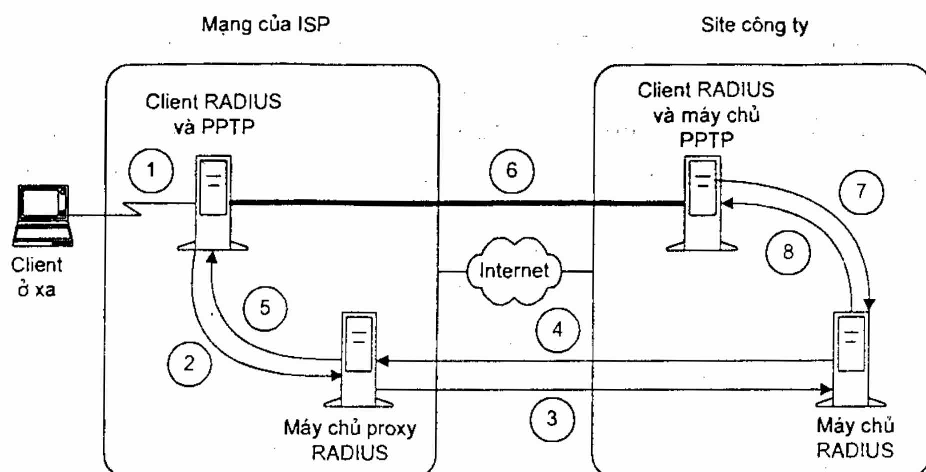
Để RADIUS có thể điều khiển việc thiết lập một đường hầm, nó cần phải lưu các thuộc tính của đường hầm. Các thuộc tính này bao gồm giao thức đường hầm được sử dụng (PPTP hay L2TP), địa chỉ của máy chủ và môi trường truyền dẫn trong đường hầm được sử dụng.

Khi kết hợp đường hầm động với RADIUS, ít nhất là có 3 tuỳ chọn cho việc xác thực và cấp quyền:

- Xác thực và nhận cấp quyền một lần tại RAS đặt tại cuối đường hầm.

- Xác thực và nhận cấp quyền một lần tại RAS đặt tại cuối đường hầm và cố gắng chuyển đáp ứng của RADIUS đến đầu xa của đường hầm.
- Xác thực tại 2 đầu của đường hầm.

Tuỳ chọn thứ nhất độ tin cậy rất kém do nó chỉ yêu cầu một mình ISP điều khiển tiến trình truy cập mạng. Tuỳ chọn thứ hai có độ tin cậy trung bình, nó phụ thuộc cách RADIUS trả lời xác thực. Tuỳ chọn thứ ba có độ tin cậy cao và làm việc tốt nếu như sử dụng máy chủ proxy RADIUS.



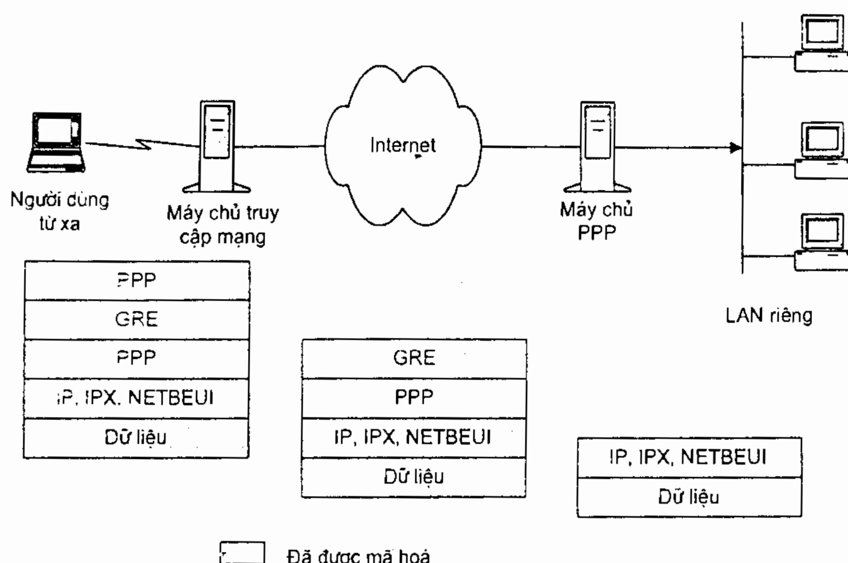
Hình 6.7: RADIUS xác thực cho các đường hầm động

Hình 6.7 mô tả tiến trình tạo đường hầm khi sử dụng RADIUS. Đầu tiên người dùng ở xa sẽ quay số truy cập vào máy chủ truy cập từ xa, gõ vào mật khẩu (bước 1 trong hình). Máy chủ truy cập từ xa đóng vai trò như một RADIUS client, sử dụng RADIUS để kiểm tra mật khẩu và nhận thông tin đường hầm từ máy chủ proxy RADIUS nội bộ. Thông tin này bao gồm các thuộc tính của máy chủ PPTP ở đầu bên kia (từ bước 2 đến bước 5). Máy chủ truy cập từ xa sẽ mở kết nối đường hầm và tạo đường hầm nếu cần thiết. Cần lưu ý là nhiều người dùng có thể truyền dữ liệu trên cùng một đường hầm bắt buộc tại cùng một thời điểm. Máy chủ PPTP sẽ xác thực lại (bước 6), kiểm tra lại mật khẩu lấy từ máy chủ RADIUS (bước 7, 8). Sau khi xác thực, máy chủ PPTP sẽ chấp nhận các gói đường hầm từ người dùng và chuyển chúng tới máy đích nằm trong mạng.

6.1.4 Xác thực và mã hoá

Các client PPTP được xác thực cũng tương tự như các client RAS được xác thực từ máy chủ PPP. Công cụ RRAS của Microsoft hỗ trợ xác thực CHAP, PAP.

MS-CHAP. MS-CHAP sử dụng hàm băm MD4 để tạo thẻ bài thách đố từ mật khẩu của người dùng. PAP và CHAP có khuyết điểm là cả hai dựa trên mật khẩu lưu tại máy đầu xa và tại máy cục bộ. Nếu như máy tính bị điều khiển bởi kẻ tấn công từ mạng thì mật khẩu sẽ bị thay đổi. Với PAP và CHAP không thể gán các đặc quyền truy cập mạng khác nhau cho những người dùng khác nhau tại cùng một máy tính từ xa. Bởi vì khi cấp quyền đã được gán cho một máy tính thì mọi người dùng tại máy tính đó đều có đặc quyền truy cập mạng như nhau.



Hình 6.8 Mã hoá gói trong PPTP

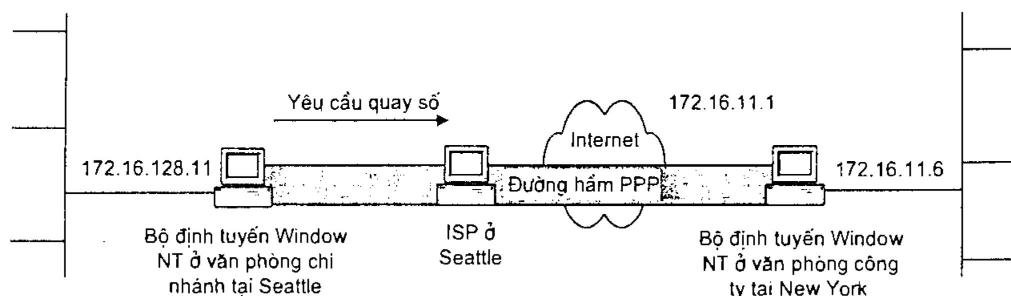
Với các công cụ PPTP của Microsoft thì dữ liệu được mã hoá theo mã hoá điểm-điểm của Microsoft - MPPE (Micosoft Point-to-Point Encryption). Phương thức này dựa trên chuẩn RSA RC4 (hình 6.8). Giao thức điều khiển nén CCP (Compression Control Protocol) được sử dụng bởi PPP để thoả hiệp việc mã hoá. MS-CHAP được dùng để kiểm tra tính hợp lý người dùng cuối tại tên miền Window NT. Một khoá phiên 40 bit được sử dụng cho mã hoá nhưng người dùng tại Mỹ có thể cài đặt một phần mềm nâng cấp lên đến 128 bit. Bởi vì MPPE mã hoá các gói PPP tại client trước khi chuyển chúng vào đường hầm PPTP nên các gói được bảo mật từ trạm làm việc đến máy chủ PPTP của máy mà nó muốn làm việc. Việc thay đổi khoá phiên có thể được thoả thuận lại sau mỗi gói hay sau một số gói.

6.1.5 Đường hầm kết nối LAN-LAN

Giao thức PPTP nguyên thủy chỉ tập trung hỗ trợ cho việc quay số kết nối vào một VPN thông qua mạng Internet, nhưng đường hầm kết nối LAN-LAN

không được hỗ trợ. Mãi đến khi Microsoft giới thiệu máy chủ định hướng và truy cập từ xa (Routing and Remote Access Server) cho NT server 4.0 thì mới hỗ trợ đường hầm kết nối LAN-LAN. Kể từ đó các nhà cung cấp khác cũng đã cung cấp các máy chủ tương thích với PPTP có hỗ trợ đường hầm kết nối LAN-LAN.

Đường hầm kết nối LAN-LAN diễn ra giữa 2 máy chủ PPTP, giống như IPSec dùng 2 cổng nối bảo mật để kết nối 2 mạng LAN. Tuy nhiên do trong kiến trúc PPTP không có hệ thống quản lý khoá nên việc cấp quyền và xác thực được điều khiển bởi CHAP hoặc thông qua MS-CHAP. Để tạo đường hầm giữa 2 site, máy chủ PPTP tại một site sẽ được xác thực bởi PPTP ở site kia. Khi đó máy chủ PPTP trở thành client PTP của PPTP ở đầu bên kia và ngược lại, do đó một đường hầm tự nguyện được tạo ra giữa 2 site.

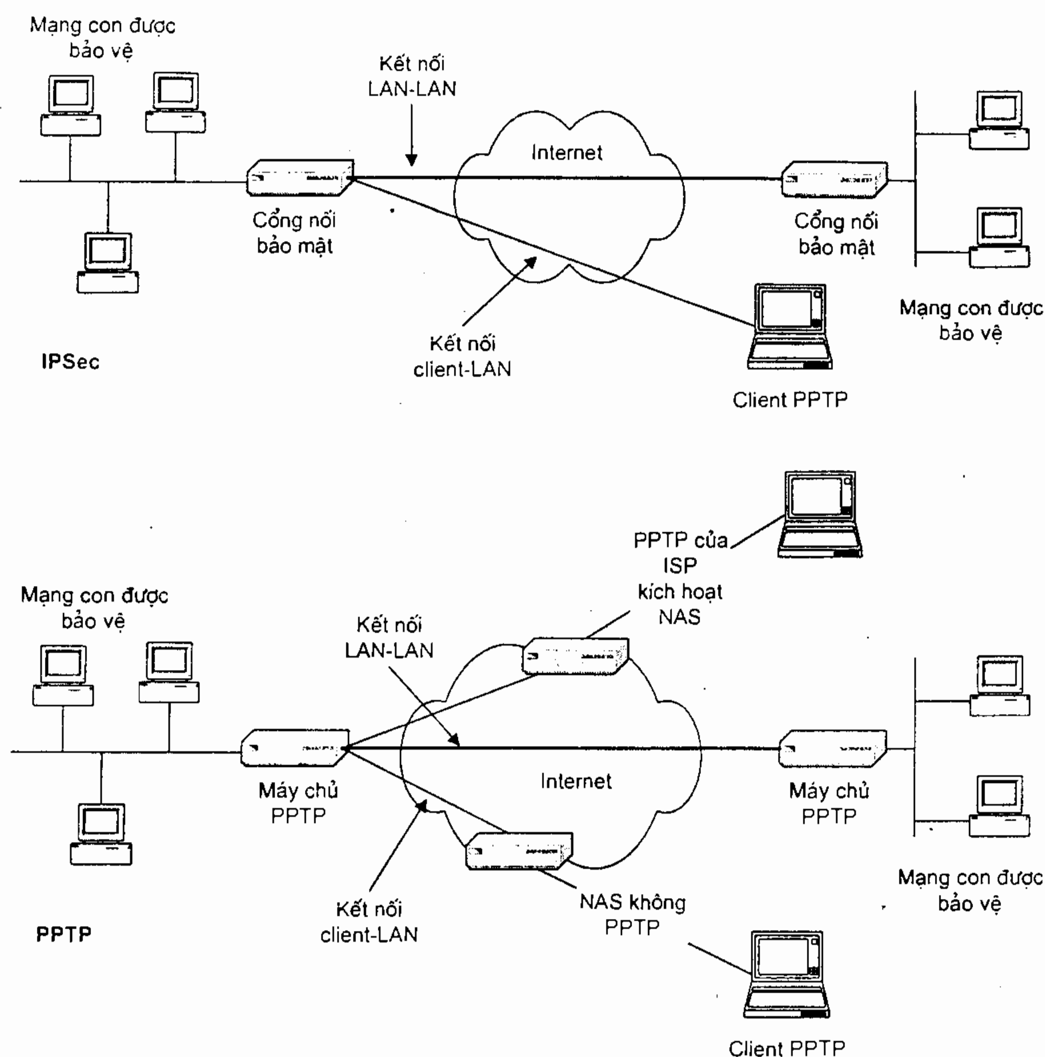


Hình 6.9 Đường hầm PPTP kết nối LAN-LAN

Do đường hầm này được đóng gói bởi bất kỳ giao thức mạng nào được hỗ trợ (IP, IPX, NETBEUI), người dùng tại một site có thể truy cập vào tài nguyên tại site kia dựa trên quyền truy cập của họ. Điều này có nghĩa cần có site quản lý để đảm bảo một người dùng tại một site có quyền truy cập vào site kia. Trong Windows NT mỗi site sẽ có miền bảo mật riêng và các site phải thiết lập một mối quan hệ tin cậy giữa các miền để cho phép người dùng truy cập vào tài nguyên của các site.

6.2 Sử dụng PPTP

Do đặc điểm chủ yếu của PPTP là cung cấp phương thức quay số truy cập bảo mật vào VPN nên các bộ phận của PPTP VPN được tổ chức có hơi khác với IPSec VPN. Điều quan trọng nhất trong PPTP là việc định nghĩa điểm kết thúc của đường hầm. Bởi vì một trong các điểm kết thúc này có thể nằm ở thiết bị của nhà cung cấp dịch vụ Internet, cấu hình này đòi hỏi phải có hợp tác giữa ISP và người quản lý mạng trong việc xác thực người dùng.



Hình 6.10 So sánh kiến trúc IPSec và PPTP

Tổng quát PPTP yêu cầu phải có: một máy chủ truy cập mạng (NAS), một máy chủ PPTP và một client PPTP. Mặc dù máy chủ PPTP có thể cài đặt tại máy của công ty và do một nhóm người của công ty quản lý nhưng NAS phải do ISP hỗ trợ thì mới có được.

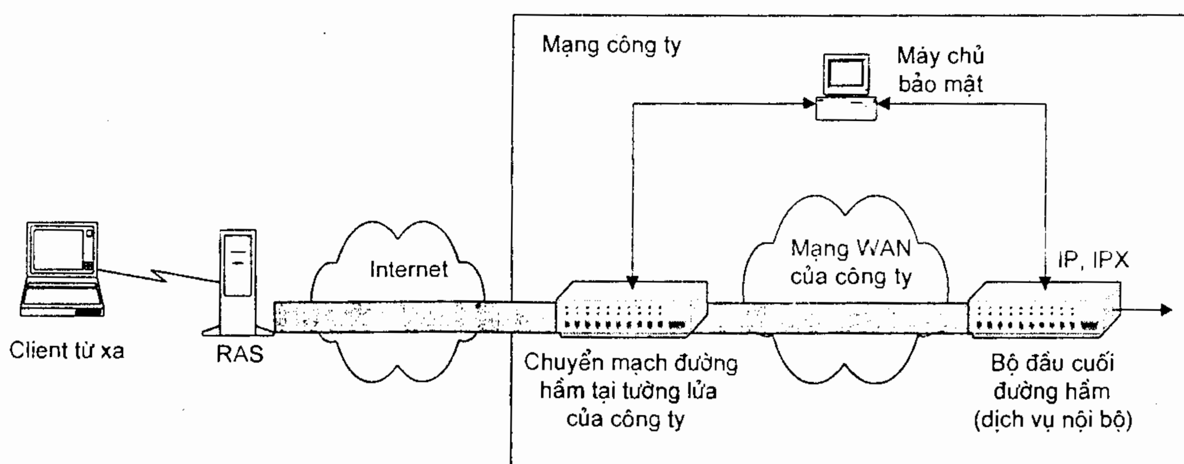
Hình 6.10 minh họa điểm khác biệt giữa cấu trúc một IPSec VPN và PPTP VPN. Một điểm khác biệt quan trọng đó là PPTP cho phép khả năng không phụ thuộc một số chức năng PPTP của ISP. Tại site cùng làm việc, máy chủ PPTP đóng vài trò như một cổng nối bảo mật nối kết xác thực với RADIUS hay các miền Windows NT. Client PPTP tại máy tính xách tay của người dùng có thể thực thi những chức năng giống như phần mềm client IPSec.

6.2.1 Máy chủ PPTP

Một máy chủ PPTP có 2 vai trò chính là: nó đóng vai trò là điểm kết thúc của đường hầm PPTP và chuyển các gói đến từ đường hầm đến mạng LAN riêng. Máy chủ PPTP chuyển các gói đến các máy đích bằng cách xử lý gói PPTP để có được địa chỉ mạng của máy tính đích.

PPTP cũng có khả năng lọc các gói bằng cách sử dụng lọc PPTP. Lọc PPTP có thể cho phép máy chủ ngăn cấm chỉ cho phép truy cập vào Internet, mạng cục bộ hay cả hai. Trong hệ thống như Windows NT và RRAS thì kết hợp giữa lọc PPTP và lọc IP cho phép tạo chức năng tường lửa cho mạng.

Thiết lập một máy chủ PPTP tại site mang lại một ít giới hạn đặc biệt nếu như máy chủ PPTP nằm sau tường lửa. PPTP được thiết kế sao cho chỉ có một cổng TCP/IP được sử dụng để chuyển dữ liệu đi, cổng đó là 1723. Sự khiếm khuyết của cấu hình cổng này có thể làm cho tường lửa dễ bị tấn công hơn. Nếu như tường lửa được cấu hình để lọc gói thì phải thiết lập cho nó cho phép GRE đi qua.



Hình 6.11: Ví dụ sử dụng chuyển mạch đường hầm

Một thiết bị tương tự khác là chuyển mạch đường hầm. Chuyển mạch đường hầm được khởi xướng từ năm 1998 bởi hãng 3Com. Mục đích của việc chuyển mạch đường hầm là mở rộng đường hầm từ một mạng đến một mạng khác, trải rộng đường hầm từ mạng của ISP đến mạng riêng (hình 6.11). Chuyển mạch đường hầm có thể được sử dụng tại tường lửa làm tăng khả năng quản lý truy cập từ xa vào tài nguyên của mạng nội bộ, nó có thể kiểm tra các gói đến về giao thức của các khung PPP hoặc tên của người dùng từ xa.

6.2.2 Phần mềm client PPTP

Nếu như các thiết bị của ISP đã hỗ trợ PPTP thì không cần phần cứng hay phần mềm nào cho các client; chỉ cần kết nối chuẩn PPP là đủ. Nếu như các thiết bị của ISP không hỗ trợ PPTP thì một client Windows NT (hoặc các phần mềm tương tự) vẫn có thể tạo kết nối bảo mật bằng cách: đầu tiên quay số kết nối với ISP bằng PPP, sau đó quay số một lần nữa thông qua cổng PPTP ảo được thiết lập ở client.

Client PPTP đã có sẵn ở Win9x và Windows NT. Hãng Network Telesystem cũng đưa ra client PPTP cho tất cả các máy phổ biến bao gồm cả máy Mac. Khi chọn client PPTP cần phải so sánh các chức năng của nó với máy chủ PPTP đã có. Không phải tất cả mọi phần mềm client đều hỗ trợ MS-CHAP, nếu thiếu công cụ này thì không thể tận dụng được ưu điểm mã hoá của Microsoft trong RRAS.

6.2.3 Máy chủ truy cập mạng RAS

Không giống như IPSec VPN, có nhiều trường hợp để thiết kế PPTP VPN tùy theo giao thức được hỗ trợ bởi ISP. Việc hỗ trợ này đặc biệt rất quan trọng trong trường hợp người dùng di động muốn sử dụng client PPTP nhưng không có sẵn client PPTP.

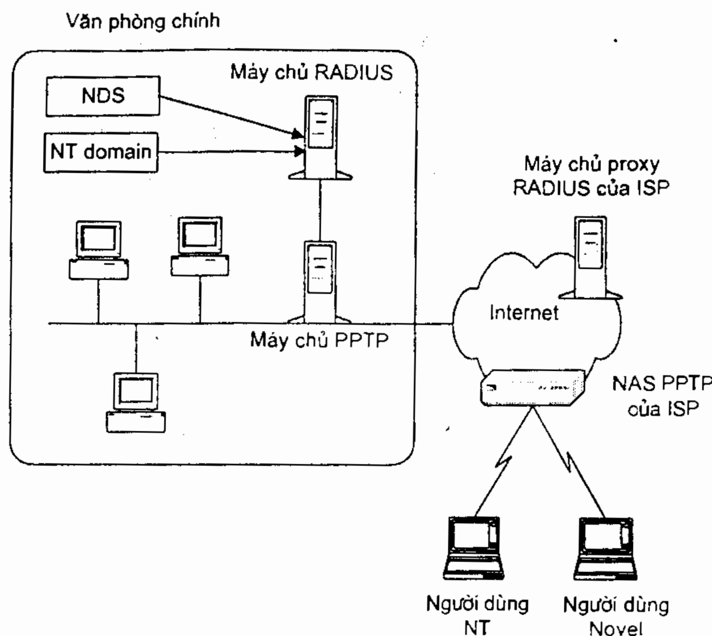
Bởi vì các ISP có thể cung cấp các dịch vụ PPTP mà không cần phải thêm hỗ trợ PPTP vào máy chủ truy cập của họ, điều này đòi hỏi tất cả người dùng phải có client PPTP tại máy của họ. Điều này mang lại ưu điểm là người dùng có thể sử dụng dịch vụ của nhiều ISP khi mô hình mạng của họ rộng lớn về mặt địa lý.

NAS còn có tên gọi khác là máy chủ truy cập từ xa (Remote Access Server) hay bộ tập trung truy cập (Access Concentrator), cung cấp khả năng truy cập đường dây dựa trên phần mềm và có khả năng tính cước, chạy trên nền rất mạnh và có khả năng chịu đựng lỗi tại ISP POP. NAS của ISP được thiết kế cho phép một số lượng lớn các người dùng có thể quay số truy cập vào cùng một lúc. Nếu một ISP cung cấp dịch vụ PPTP thì cần phải cài một NAS cho phép PPTP để hỗ trợ cho các client PPTP chạy trên các nền khác nhau như Unix, Windows, Macintosh. Trong các trường hợp như thế máy chủ ISP đóng vai trò như một client PPTP kết nối với máy chủ PPTP tại mạng riêng. Khi đó máy chủ ISP trở thành một điểm cuối của đường hầm điểm kết thúc còn lại là máy chủ tại đầu mạng riêng.

6.2.4 Một ví dụ minh hoạ ứng dụng PPTP trong VPN

Trong ví dụ này có 2 phần: phần 1 là minh hoạ khả năng quay số truy cập (hình 6.12) và phần 2 là minh họa cho VPN kết nối LAN-LAN (hình 6.13). Trong ví dụ này chỉ có 2 site, một ở văn phòng chính và một ở văn phòng chi nhánh.

Trong cả 2 trường hợp, chỉ đề cập đến việc trao đổi dữ liệu giữa 2 điểm cuối. không quan tâm đến thông tin trong mạng được bảo mật như thế nào (sử dụng tường lửa chẳng hạn). Các host được nối tới máy chủ PPTP và mỗi ngõ đi ra ngoài đều phải thông qua máy chủ PPTP kết hợp với tường lửa. Kết nối giữa site trong mạng và site bên ngoài phải được khoá lại sao cho chỉ có người quản trị mạng mới truy cập tới được máy chủ mã hoá.

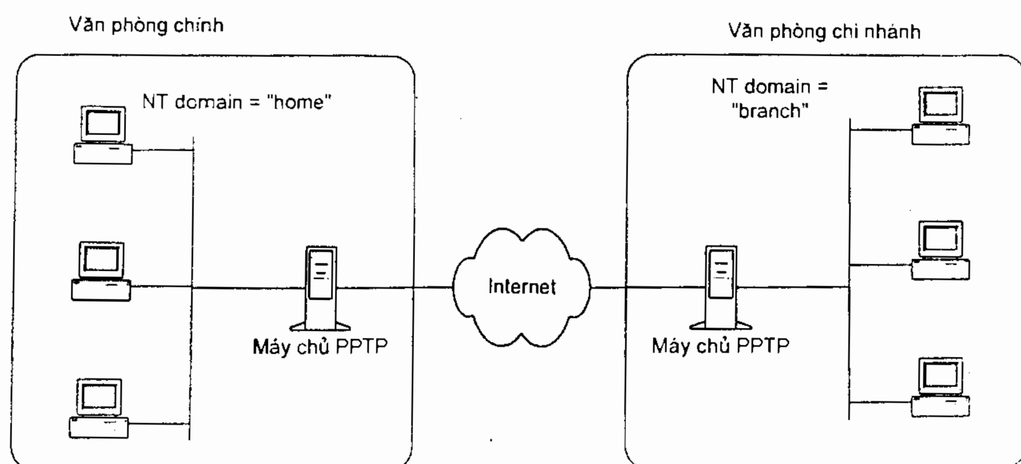


Hình 6.12: PPTP quay số truy cập VPN

Trong ví dụ hình 6.12, công ty A quyết định sử dụng dịch vụ VPN có sự hỗ trợ của ISP. Điều này có nghĩa là ISP cung cấp kết nối Internet cho công ty A có máy chủ proxy RADIUS và NAS có hỗ trợ PPTP. Ở tại công ty A vẫn có duy trì máy chủ RADIUS và máy chủ PPTP. Do ISP có hỗ trợ PPTP nên các máy đầu xa không cần phải cài client PPTP. Sử dụng server RADIUS để điều khiển xác thực và quyền truy cập cho phép công ty A khả năng điều khiển truy cập tập trung, điều này đặc biệt hữu ích khi làm việc trong môi trường đa giao thức.

Trong ví dụ hình 6.13 một máy chủ Windows NT được đặt tại mỗi site để phục vụ cho bộ định tuyến và máy chủ PPTP. Để 2 site này có thể liên lạc được với nhau thông qua đường hầm PPTP thì máy chủ PPTP của một site phải cấu hình trở thành client PPTP của máy chủ PPTP site bên kia. Nếu như 2 site kết nối với nhau bằng cách quay số thay vì có một kết nối mạng thường trực thì địa chỉ IP của NAS của ISP phải nằm trong cấu hình.

Khi có luồng dữ liệu cần truyền cho văn phòng chính thì máy chủ PPTP chi nhánh sẽ đóng vai trò là client PPTP và sẽ tạo một đường hầm, nếu như chưa tồn tại, đến PPTP ở văn phòng chính để truyền dữ liệu. Nếu như văn phòng chính có luồng dữ liệu truyền cho chi nhánh thì quá trình sẽ ngược lại.



Hình 6.13: Dùng PPTP trong VPN kết nối LAN-LAN

6.3 Khả năng áp dụng trong thực tế

PPTP là một giải pháp tạm thời bởi vì hầu hết các nhà cung cấp đều có kế hoạch thay thế PPTP bằng L2TP khi mà giao thức đã được chuẩn hoá. PPTP thích hợp cho quay số truy cập với một lượng người dùng giới hạn hơn là cho VPN kết nối LAN-LAN. Một vấn đề của PPTP là xử lý xác thực quyền người dùng thông qua Windows NT hay thông qua RADIUS. Máy chủ PPTP cũng quá tải đối với một số lượng người dùng quay số truy cập hay một lưu lượng lớn dữ liệu truyền qua, mà điều này là một yêu cầu của kết nối LAN-LAN. Khi sử dụng VPN PPTP mà có hỗ trợ thiết bị của ISP thì một số quyền quản lý phải chia sẻ cho ISP. Tính bảo mật của PPTP không mạnh bằng IPSec. Nói một cách khác việc quản lý bảo mật trong PPTP lại ít phức tạp.

CHƯƠNG 7

GIAO THỨC L2TP

Giao thức định đường hầm lớp 2 L2TP (Layer 2 Tunneling Protocol) là sự kết hợp giữa 2 giao thức đó là PPTP và chuyển tiếp lớp 2 - L2F (Layer 2 Forwarding). PPTP do Microsoft đưa ra còn L2F do Cisco khởi xướng. Hai công ty này đã hợp tác cùng kết hợp 2 giao thức lại và đăng ký chuẩn hoá tại IETF.

Giống như PPTP, L2F là giao thức đường hầm, nó sử dụng tiêu đề đóng gói riêng cho việc truyền các gói ở lớp 2. Một điểm khác biệt chính giữa L2F và PPTP là L2F không phụ thuộc vào IP và GRE, cho phép nó có thể làm việc ở môi trường vật lý khác. Bởi vì GRE không sử dụng như giao thức đóng gói, nên L2F định nghĩa riêng cách thức các gói được điều khiển trong môi trường khác. Tương tự như PPTP, L2F tận dụng PPP để xác thực người dùng quay số truy cập. Nhưng nó cũng hỗ trợ TACACS+ và RADIUS cho việc xác thực. Có 2 mức xác thực người dùng: đầu tiên ở ISP trước khi thiết lập đường hầm, sau đó là ở cổng nối của mạng riêng sau khi kết nối được thiết lập.

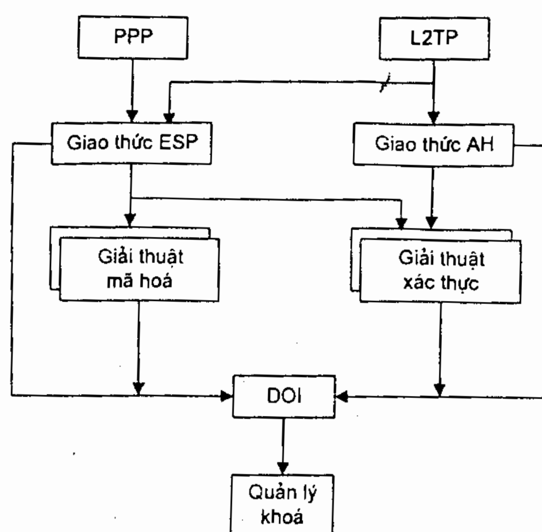
L2TP mang các đặc tính của PPTP và L2F. Tuy nhiên L2TP định nghĩa riêng một giao thức đường hầm dựa trên hoạt động của L2F. Nó cho phép L2TP truyền thông qua nhiều môi trường gói khác nhau như X.25, Frame Relay, ATM. Mặc dù nhiều công cụ chủ yếu của L2TP tập trung cho UDP của mạng IP, nhưng có thể thiết lập một hệ thống L2TP mà không cần phải sử dụng IP làm giao thức đường hầm. Một mạng ATM hay Frame Relay có thể áp dụng cho đường hầm L2TP.

Do L2TP là giao thức ở lớp 2 nên nó cho phép người dùng sử dụng các giao thức điều khiển một cách mềm dẻo không chỉ là IP mà có thể là IPX hoặc NETBEUI. Cũng giống như PPTP, L2TP cũng có cơ chế xác thực PAP, CHAP hay RADIUS.

Mặc dù Microsoft đã làm cho PPTP trở nên cách chọn lựa phổ biến khi xây dựng VPN bằng cách hỗ trợ giao thức này sẵn trong ệ điều hành Windows

nhưng công ty cũng có kế hoạch hỗ trợ thêm L2TP trong Windows NT 4.0 và Windows 98.

7.1 Dạng thức của L2TP



Hình 7.1: Kiến trúc của L2TP

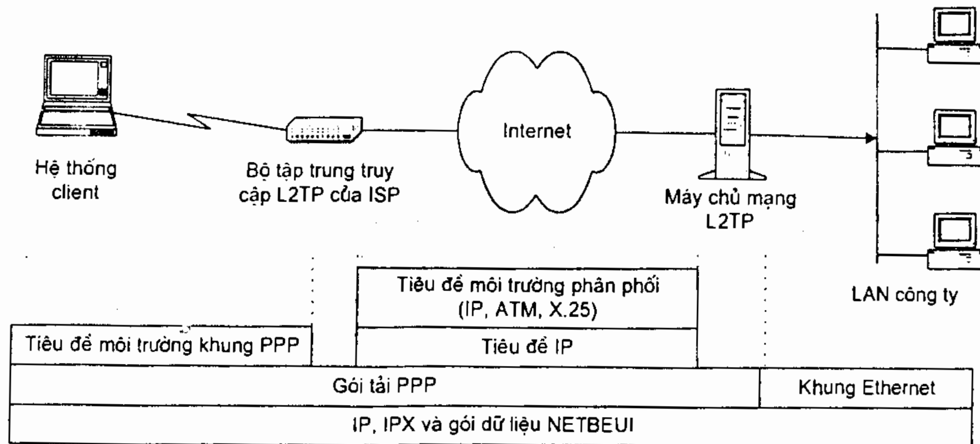
Những phần chính của L2TP bao gồm: giao thức điểm-điểm, đường hầm và hệ thống xác thực. Tuy nhiên để tăng thêm độ bảo mật thì L2TP cũng sử dụng quản lý khoá giống như IPSec. Hình 7.1 mô tả kiến trúc của L2TP.

7.1.1 PPP và L2TP

L2TP dựa trên PPP để tạo kết nối quay số giữa client và máy chủ truy cập mạng (NAS).

L2TP sử dụng PPP để tạo kết nối vật lý, tiến hành giai đoạn xác thực đầu, tạo gói dữ liệu PPP và đóng kết nối khi kết thúc phiên làm việc.

Sau khi PPP tạo kết nối xong, L2TP sẽ xác định NAS tại site chính có chấp nhận người dùng và sẵn sàng đóng vai trò là điểm kết thúc đường hầm cho người dùng đó. Sao khi đường hầm được tạo, L2TP sẽ đóng gói các gói PPP rồi truyền lên môi trường mà ISP đã gán cho đường hầm đó (hình 7.2). L2TP tạo đường hầm giữa NAS của ISP và máy chủ mạng của client, nó có thể gán nhiều phiên làm việc cho đường hầm. L2TP tạo ra các số nhận dạng cuộc gọi (Call ID) cho mỗi phiên làm việc và chèn Call ID vào tiêu đề L2TP của mỗi gói để chỉ ra nó thuộc phiên làm việc nào.



Hình 7.2: Các giao thức sử dụng trong một kết nối L2TP

L2TP cũng có thể tạo nhiều đường hầm giữa NAS của ISP và máy chủ mạng của client. Bằng việc chọn gán một phiên làm việc của người dùng cho một đường hầm thay vì ghép nhiều phiên làm việc vào một đường hầm, cho phép gán các người dùng khác nhau vào các môi trường đường hầm tuỳ theo chất lượng dịch vụ của họ.

Giống như PPTP, L2TP cũng định nghĩa 2 loại thông báo đó là thông báo điều khiển và thông báo dữ liệu. Tuy nhiên không giống như PPTP, L2TP truyền cả 2 loại thông báo chung trên một luồng. Nếu như đường hầm được dùng cho truyền trên mạng IP thì cả 2 loại thông báo đều được gửi trên cùng gói dữ liệu UDP.

Thông báo điều khiển L2TP điều khiển việc thiết lập, quản lý và giải phóng phiên làm việc trên đường hầm.

Do L2TP làm việc ở lớp thứ 2 nên trong thông báo dữ liệu L2TP bao gồm tiêu đề môi trường để chỉ ra đường hầm làm việc trong môi trường nào (hình 7.3). Tuỳ theo nhà ISP mà môi trường có thể là Ethernet, X.25, Frame Relay, ATM hay liên kết PPP.

Môi trường	L2TP	PPP	Tải PPP

Hình 7.3: Bọc gói L2TP

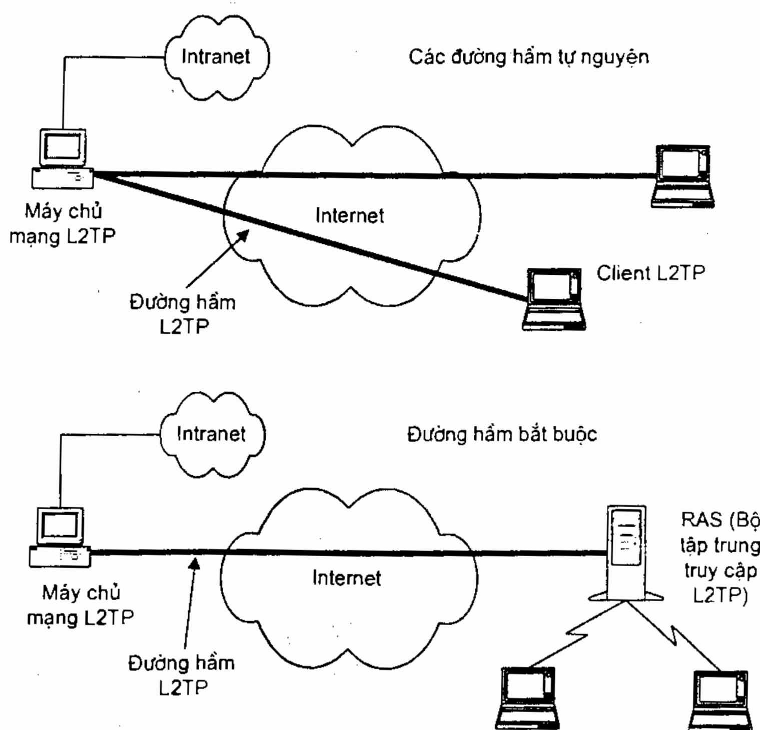
L2TP cũng giúp đỡ làm giảm tải trên mạng, nó giúp máy chủ giải quyết tắc nghẽn bằng cơ chế điều khiển luồng giữa NAS, theo thuật ngữ gọi là bộ tập trung truy cập L2TP - LAC (L2TP Access Concerntrator) và máy chủ của mạng riêng,

theo thuật ngữ gọi là máy chủ mạng L2TP - LNS (L2TP Network Server). Thông báo điều khiển cho biết tốc độ truyền và tham số của bộ đệm dùng để điều khiển luồng các gói PPP trong một phiên làm việc.

7.1.2 Đường hầm L2TP

L2TP sử dụng những lớp đường hầm tương tự như PPTP (các đường hầm tự nguyện và bắt buộc) tuỳ theo người dùng sử dụng client PPP hay client L2TP để khởi tạo kết nối.

Đường hầm tự nguyện được tạo theo yêu cầu của người dùng cho mục đích sử dụng cụ thể. Đường hầm bắt buộc được tạo tự động không cần bất kỳ hành động nào từ phía người dùng và đặc biệt là không cho phép người dùng có sự chọn lựa nào.



Hình 7.4: Các đường hầm tự nguyện và bắt buộc

Khi người dùng sử dụng đường hầm tự nguyện thì có thể đồng thời mở đường hầm bảo mật thông qua Internet và vừa có thể truy cập vào một host bất kỳ trên Internet theo giao thức TCP/IP bình thường. Điểm kết thúc đường hầm của đường hầm tự nguyện nằm ở máy tính người dùng. Đường hầm tự nguyện thường được sử dụng để cung cấp tính riêng tư và toàn vẹn dữ liệu cho lưu lượng Intranet được gửi thông qua Internet.

Do đường hầm bắt buộc được tạo ra không thông qua người dùng nên nó trong suốt đối với người dùng đầu cuối. Điểm kết thúc của đường hầm bắt buộc nằm ở LAC của ISP. Tất cả dữ liệu truyền đi từ người dùng qua đường hầm L2TP thông qua LAC. Truy cập vào những dịch vụ khác ngoài Intranet cần phải thông qua nhà quản lý mạng. Cần lưu ý là L2TP cho phép đa kết nối cùng tải trên một đường hầm, điều này làm tăng dung lượng cho L2TP.

Bởi vì đường hầm bắt buộc định trước điểm kết thúc và người dùng không thể truy cập phần còn lại của Internet nên nó điều khiển truy cập tốt hơn là đường hầm tự nguyện. Nếu như vì tính bảo mật mà không cho người dùng truy cập Internet công cộng thì đường hầm bắt buộc ngăn không cho họ truy cập Internet công cộng nhưng vẫn cho phép dùng Internet để truy cập VPN (nghĩa là chỉ truy cập vào được các site trong VPN mà thôi).

Một ưu điểm nữa của đường hầm bắt buộc là một đường hầm có thể tải nhiều kết nối. Đặc tính này làm giảm yêu cầu băng thông mạng cho các ứng dụng đa phiên làm việc. Một khuyết điểm của đường hầm bắt buộc là kết nối từ LAC đến người dùng nằm ngoài đường hầm nên dễ bị tấn công. Điều này là một trong những lý do L2TP sử dụng một số đặc điểm của IPSec để bảo mật lưu lượng.

Mặc dù ISP có thể chọn cách thiết lập tĩnh để định nghĩa đường hầm cho người dùng, nhưng điều này sẽ làm lãng phí tài nguyên của mạng nếu như đường hầm tĩnh đó không được sử dụng thường xuyên. Có cách khác mềm dẻo hơn đó là chọn đường hầm động khi mà người dùng kết nối với RAS hay LAC, cho phép sử dụng tài nguyên của mạng hiệu quả hơn. Những đường hầm động này được thiết lập trong L2TP bằng cách kết nối hệ thống với máy chủ RADIUS

Sử dụng RADIUS để cung cấp đường hầm bắt buộc có một vài ưu điểm. Các đường hầm có thể được định nghĩa và kiểm tra dựa trên xác thực người dùng và tính cước có thể dựa trên số điện thoại, hoặc các phương thức xác thực khác, chẳng hạn như thẻ bài hay card thông minh. Để RADIUS có thể điều khiển việc thiết lập một đường hầm, nó cần phải lưu các thuộc tính của đường hầm. Các thuộc tính này bao gồm giao thức đường hầm được sử dụng (PPTP hay L2TP), địa chỉ của máy chủ và môi trường truyền dẫn trong đường hầm được sử dụng.

7.1.3 Xác thực và mã hoá trong L2TP

Việc xác thực người dùng diễn ra trong 3 giai đoạn: giai đoạn 1 diễn ra tại ISP, giai đoạn 2 và giai đoạn 3 (tuỳ chọn) diễn ra ở máy chủ của mạng riêng.

Trong giai đoạn đầu, ISP có thể sử dụng số điện thoại của người dùng hoặc tên người dùng để xác định dịch vụ L2TP được yêu cầu và khởi tạo kết nối đường hầm đến máy chủ của mạng riêng. Khi đường hầm được thiết lập, LAC của ISP

phải chỉ định một số nhận dạng cuộc gọi (Call ID) mới để định danh cho kết nối trong đường hầm và khởi tạo phiên làm việc bằng cách chuyển thông tin xác thực đến máy chủ của mạng riêng.

Máy chủ của mạng riêng sẽ tiến hành tiếp bước thứ 2 là quyết định có chấp nhận hay từ chối cuộc gọi. Cuộc gọi từ ISP chuyển đến có thể mang CHAP, PAP, EAP hay bất kỳ thông tin xác thực nào, máy chủ sẽ dựa vào các thông tin này để quyết định chấp nhận hay từ chối cuộc gọi này.

Sau khi cuộc gọi được chấp nhận thì máy chủ mạng có thể khởi động giai đoạn thứ 3 của việc xác thực tại lớp PPP. Bước này tương tự như máy chủ xác thực một người dùng quay số truy cập vào thẳng máy chủ.

Mặc dầu 3 giai đoạn này cho phép người dùng, ISP và máy chủ của mạng riêng xác định được tính chính xác của cuộc gọi nhưng vẫn chưa bảo mật cho dữ liệu tránh khỏi bị can thiệp và sửa đổi.

Giữa 2 đầu cuối của đường hầm xác thực luồng qua lại lẫn nhau trong suốt quá trình thiết lập đường hầm. Cơ chế xác thực cũng tương tự như thuộc tính bảo mật của CHAP bảo mật chống lại các vụ tấn công trong suốt tiến trình thiết lập đường hầm. Tuy nhiên nó vẫn còn đơn giản cho kẻ tấn công xen vào và chiếm đường hầm ngay khi quá trình xác thực đường hầm vừa mới hoàn tất.

Mặc dầu xác thực L2TP cho phép xác thực qua lại lẫn nhau giữa LAC và LNS trong suốt quá trình thiết lập đường hầm nhưng nó không bảo mật cho các luồng thông báo điều khiển và thông báo dữ liệu. Sự khiếm khuyết này làm cho đường hầm dễ bị tấn công bao gồm việc chèn gói dữ liệu vào để chiếm quyền điều khiển đường hầm hay kết nối PPP, hoặc phá vỡ việc đàm phán PPP, lấy được mật khẩu người dùng...

Xác thực PPP từ client đến LNS nhưng nó không cung cấp xác thực cho gói, không toàn vẹn dữ liệu, hoặc bảo mật. Mã hoá PPP là một yêu cầu tin cậy cho luồng PPP nhưng nó không có xác thực địa chỉ, toàn vẹn dữ liệu, quản lý khoá nên làm cho nó trở thành công cụ bảo mật yếu kém, không thể giúp cho bảo mật trong kênh L2TP.

Để việc xác thực trong L2TP được như mong muốn, cần phải phân phối khoá. Mặc dù phân phối khoá bằng tay có thể khả thi trong một số trường hợp, nhưng yêu cầu phải có một giao thức quản lý khoá cho mọi trường hợp.

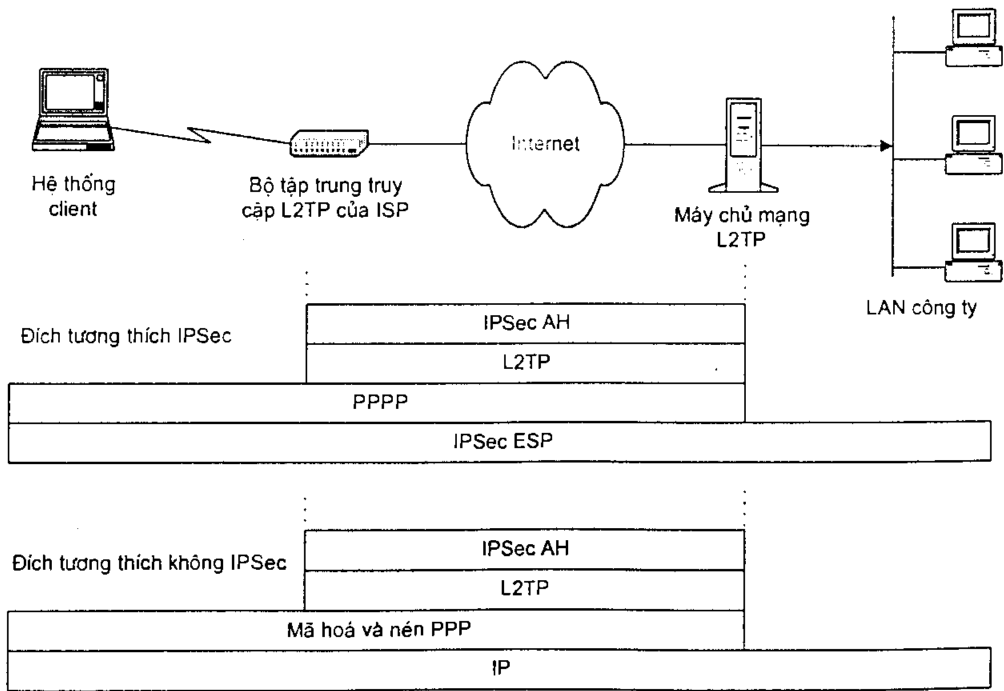
Đối với đường hầm L2TP trên IP, bảo mật gói mức IP sử dụng IPSec cung cấp khả năng bảo mật cao cho đường hầm. Việc bảo mật này không đòi hỏi phải sửa đổi giao thức L2TP.

Cần chú ý là một vài loại tấn công được tiến hành trên kết nối PPP giữa client quay số và NAS/LAC. L2TP là sẽ là một giải pháp tốt cho VPN nếu như nó

bảo mật dữ liệu đầu cuối-đầu cuối. Điều này dẫn đến phải có kế hoạch sử dụng IPSec để mã hoá các gói, tối thiểu là cho các đường hầm dựa trên IP.

Bởi vì các chức năng của ESP được định nghĩa trên tải IP nên tiêu đề IP không cần thiết cho ESP. Do đó L2TP trên các mạng không phải IP có thể chuyển được các gói ESP. Nhưng việc chuyển khoá và đàm phán SA lại là vấn đề khác. Đối với IKE, các thông báo tải trên UDP, điều này làm cho các môi trường không phải là IP phải hỗ trợ việc truyền gói dữ liệu UDP.

Hãy xem xét IPSec được thực thi như thế nào trong đường hầm tự nguyện và bắt buộc. Trong trường hợp đường hầm bắt buộc, người dùng gửi những gói PPP đến LAC mà không cần quan tâm đến đường hầm được tạo giữa LAC và LNS tại mạng riêng. Một SA được thiết lập giữa LAC và LNS dựa trên yêu cầu và danh định của người dùng và SA này chỉ được biết đến bởi LAC và LNS, người dùng không quan tâm đến.

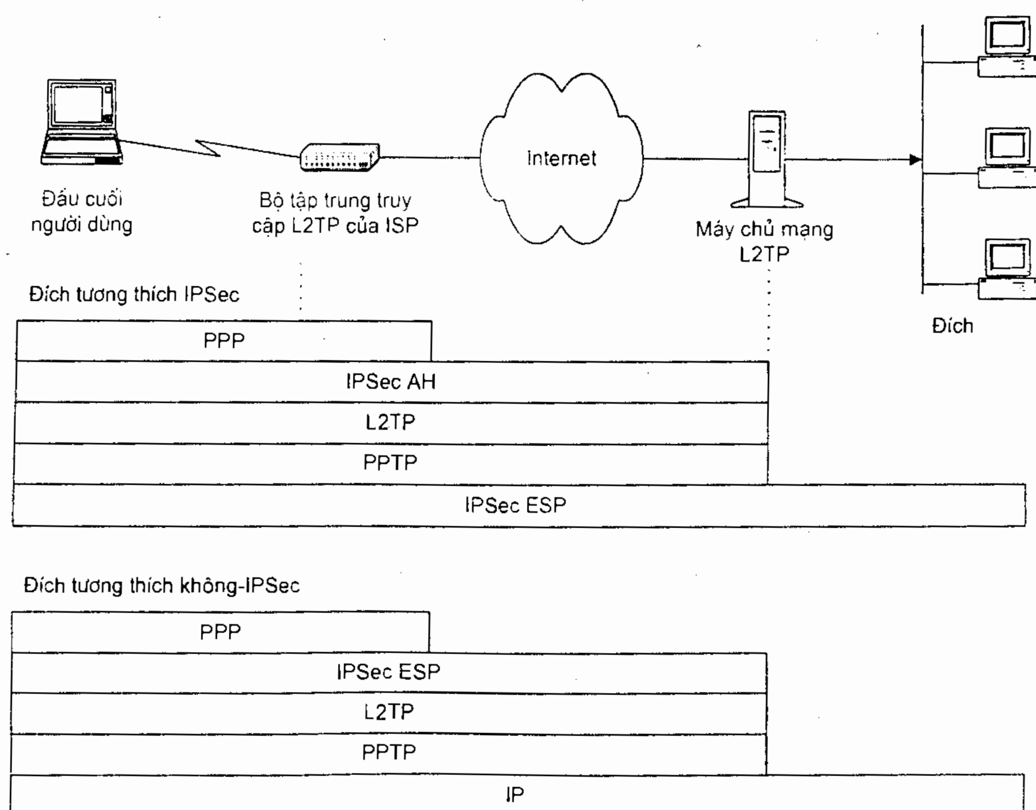


Hình 7.5: Mã hoá gói cho đường hầm bắt buộc

Do người dùng đầu cuối không quan tâm đến dịch vụ bảo mật dữ liệu nằm giữa LAC và LNS, nên cách giải quyết tốt nhất cho người dùng đầu cuối là IPSec được thực thi ngay tại máy của họ.Tuy nhiên không phải các điểm kết thúc đường hầm nào cũng tương thích IPSec, điều này có thể giải quyết bằng cách đàm phán lại chỉ sử dụng mã hoá PPP (hình 7.5). Trong cả 2 trường hợp LAC của ISP phải

chèn IPSec AH vào luồng dữ liệu nhưng lại để cho người dùng đầu cuối chọn là ESP cho đầu cuối tương thích IPSec hay mã hoá PPP cho đầu cuối tương thích không IPSec.

Trong trường hợp đường hầm tự nguyện, người dùng đóng vai trò là điểm kết thúc của đường hầm, do đó có thể tiến hành đàm phán SA với LNS tại mạng riêng. Tuy nhiên việc đàm phán lại phụ thuộc vào cả 2 đầu có tương thích với IPSec hay không (hình 7.6). Do người dùng đóng vai trò là điểm kết thúc của đường hầm nên IPSec AH được áp dụng ngay máy của họ chứ không phải trên thiết bị của ISP. Nếu như đích đến không tương thích IPSec thì mã hoá ESP chỉ bảo mật dữ liệu cho đến khi nó đến LNS của mạng riêng.



Hình 7.6: Mã hoá gói cho đường hầm tự nguyện

7.1.4 Đường hầm kết nối LAN-LAN

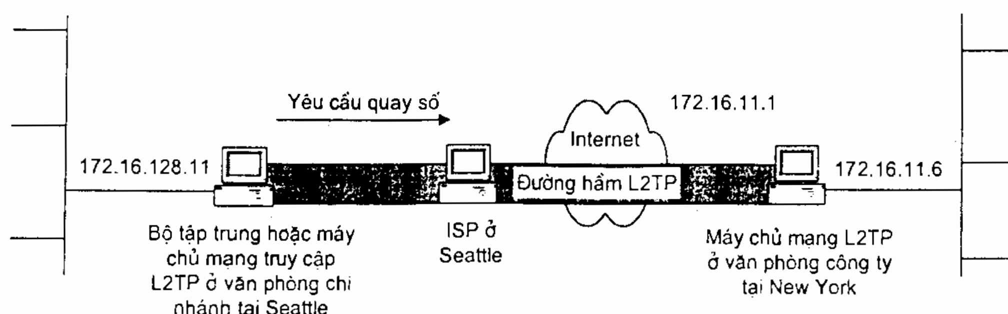
Mặc dù chức năng chính của L2TP là cho quay số truy cập VPN sử dụng client PPP, nhưng nó cũng thích hợp cho kết nối LAN-LAN trong VPN.

Đường hầm kết nối LAN-LAN được thiết lập giữa 2 máy chủ L2TP với ít nhất một trong 2 máy chủ phải có kết nối quay số tới ISP để khởi tạo phiên làm

việc PPP. Thiết kế này thích hợp cho mạng LAN của văn phòng chi nhánh kết nối vào văn phòng chính khi kết nối không cần phải duy trì thường xuyên.

Hai bên đóng vai trò vừa là LAC và LNS, khởi tạo và kết thúc đường hầm khi cần thiết (hình 7.7).

Đối với LAN kết nối vào VPN thường xuyên thông qua Internet (sử dụng Frame Relay, T1,...) cần tồn tại đường tắt trong tiến trình xác thực bởi vì RAS của ISP không đóng vai trò là LAC.



Hình 7.7: Đường hầm L2TP kết nối LAN-LAN

7.1.5 Quản lý khoá

Khi hai đối tượng muốn chuyển giao dữ liệu một cách bảo mật thì họ cần phải chắc là cả hai bên xử lý dữ liệu như nhau. Cả hai bên phải cùng sử dụng chung giải thuật mã hoá, cùng chiều dài từ khoá, cùng chung một khoá thì dữ liệu truyền mới được bảo mật. Điều này được xử lý thông qua bảo mật kết hợp SA (Security Association).

Một IPSec SA mô tả các vấn đề sau:

- Giải thuật xác thực sử dụng cho AH và khoá của nó.
- Giải thuật mã hoá ESP và khoá của nó.
- Dạng thức và kích thước của đồng bộ mật mã sử dụng trong giải thuật mã hoá.
- Giao thức. giải thuật, khoá sử dụng cho việc truyền thông.
- Giao thức, giải thuật mã hoá, khoá sử dụng cho việc truyền thông riêng.
- Bao lâu thì khoá được thay đổi.
- Giải thuật xác thực, kiểu, chức năng sử dụng trong ESP và khoá được sử dụng bởi giải thuật đó.
- Thời gian sống của khoá.

- Thời gian sống của SA.
- Địa chỉ nguồn SA.

Mặc dù SA giúp hai đối tượng truyền thông định nghĩa phương thức mã hoá mà họ sẽ thực hiện nhưng việc chuyển giao khoá lại do IKE đảm trách. IKE có các khả năng sau:

- Cung cấp các phương tiện cho hai bên thoả thuận sử dụng các giao thức, giải thuật và khoá.
- Đảm bảo ngay từ lúc bắt đầu chuyển khoá là truyền thông đúng đối tượng.
- Quản lý các khoá sau khi chúng được chấp nhận trong tiến trình thoả thuận.
- Đảm bảo các khoá được chuyển một cách bảo mật.

Chuyển khoá giống tương tự như quản lý SA. Khi cần tạo một SA cần phải chuyển khoá. Do đó cấu trúc của IKE bọc chúng lại với nhau và chuyển chúng đi như một gói tích hợp.

Bởi vì IKE dựa trên IP nên nó dễ dàng được ghép vào L2TP chạy trên mạng IP hơn là trên mạng không phải là IP.

7.2 Sử dụng L2TP

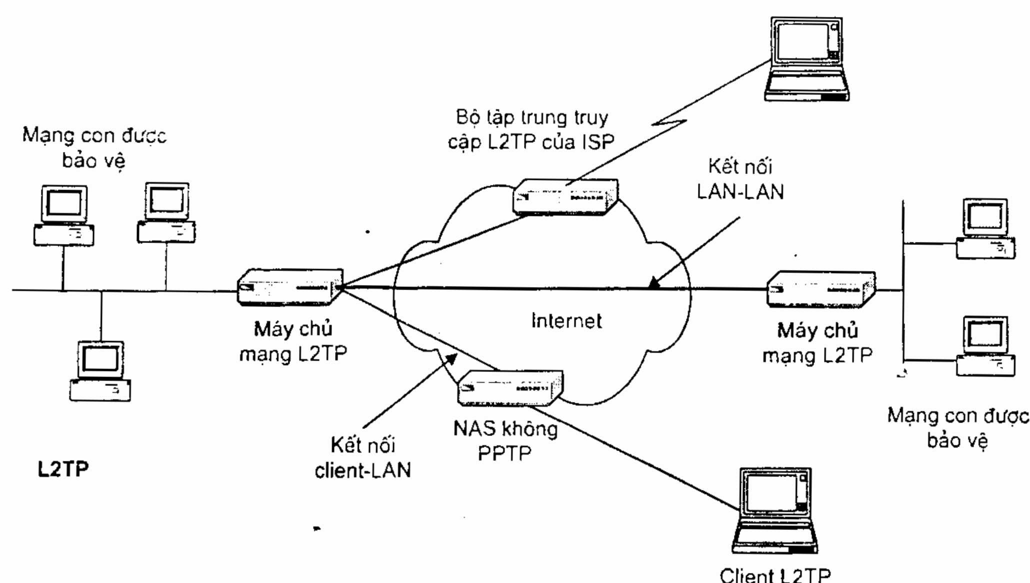
Bởi vì chức năng chính của L2TP là cho quay số truy cập VPN thông qua Internet nên các thành phần của L2TP cũng tương tự như PPTP. Thành phần quan trọng nhất của L2TP là định nghĩa điểm kết thúc một đường hầm L2TP, LAC và LNS (hình 7.8). Bởi vì các điểm này có thể nằm trên thiết bị ISP nên phần mềm cho client di động có thể không cần thiết.

Mặc dù LNS có thể thể cài đặt ngay tại công ty và điều hành bởi một nhóm làm việc của công ty, nhưng LAC nên nhờ hỗ trợ của ISP. Thực ra nếu như trên máy client từ xa có cài sẵn client L2TP thì ISP không cần phải hỗ trợ thêm L2TP.

Tại site của mạng riêng, máy chủ L2TP đóng vài trò như một cổng nối bảo mật, nối kết xác thực với RADIUS hay các miền Windows NT. Client L2TP tại máy tính xách tay của người dùng có thể thực thi những chức năng giống như phần mềm client IPSec.

7.2.1 Các máy chủ mạng L2TP

Một máy chủ L2TP có hai chức năng chính là: nó đóng vai trò là điểm kết thúc của đường hầm PPTP và chuyển các gói đến từ đường hầm đến mạng LAN riêng. Máy chủ L2TP chuyển các gói đến các máy đích bằng cách xử lý gói L2TP để có được địa chỉ mạng của máy tính đích.



Hình 7.8: Các thành phần cơ bản của L2TP

Không giống như PPTP, L2TP không có khả năng lọc các gói. Hệ thống để dành nhiệm vụ đó cho tường lửa.

Khi có tích hợp giữa máy chủ mạng và tường lửa thì L2TP có nhiều ưu điểm hơn PPTP. Trước hết, L2TP không đòi hỏi chỉ có một cổng duy nhất gán cho tường lửa như PPTP (cổng mặc định cho L2TP là 1701). Chương trình quản lý có tuỳ chọn để chọn cổng khác gán cho tường lửa, điều này gây khó khăn cho kẻ tấn công khi cố gắng tấn công vào một cổng đã biết trong khi cổng đó có thể được đổi thành một số khác. Thứ hai là luồng dữ liệu và thông tin điều khiển được truyền trên cùng một UDP, việc thiết lập tường lửa sẽ đơn giản hơn. Do một số tường lửa không có hỗ trợ GRE nên chúng tương thích với L2TP hơn là với PPTP.

7.2.2 Phần mềm client L2TP

Nếu như các thiết bị của ISP đã hỗ trợ L2TP thì không cần phần cứng hay phần mềm nào cho các client; chỉ cần kết nối chuẩn PPP là đủ. Nhưng chú ý là thiết lập trên không sử dụng được mã hoá của IPSec, điều đó có nghĩa là nên sử dụng các client tương thích L2TP cho L2TP VPN.

Sau đây là một số đặc điểm của phần mềm client L2TP:

- Tương thích với những thành phần khác của IPSec (như máy chủ mã hoá, giao thức chuyển khoá, giải thuật mã hoá, v.v...).
- Đưa ra một chỉ báo rõ ràng khi IPSec đang hoạt động.

- Hỗ trợ tải SA về.
- Hàm băm xử lý được các địa chỉ IP động.
- Có cơ chế bảo mật khoá chống lại kẻ trộm (mã hoá khoá với mật khẩu).
- Có cơ chế chuyển đổi hoá mã một cách tự động và định kỳ.
- Chặn hoàn toàn các lưu lượng không-IPSec.

7.2.3 Các bộ tập trung truy cập mạng

Không giống như IPSec VPN, trong một số trường hợp thiết kế của L2TP VPN phụ thuộc vào giao thức hỗ trợ bởi ISP. Việc hỗ trợ đặc biệt quan trọng khi các client từ xa không có client L2TP có thể sử dụng client PPP để truy cập.

Bởi vì các ISP có thể cung cấp các dịch vụ L2TP mà không cần phải thêm hỗ trợ L2TP vào máy chủ truy cập của họ, điều này đòi hỏi tất cả người dùng phải có client L2TP tại máy của họ. Điều này mang lại ưu điểm là người dùng có thể sử dụng dịch vụ của nhiều ISP khi mà mô hình mạng của họ rộng lớn về mặt địa lý.

Một ISP cung cấp dịch vụ L2TP cần phải cài một NAS cho phép L2TP để hỗ trợ cho các client L2TP chạy trên các nền khác nhau như Unix, Windows, Macintosh. Trong các trường hợp như thế ISP ACS đóng vai trò như một điểm cuối của đường hầm L2TP bắt buộc điểm kết thúc còn lại là máy chủ tại đầu mạng riêng.

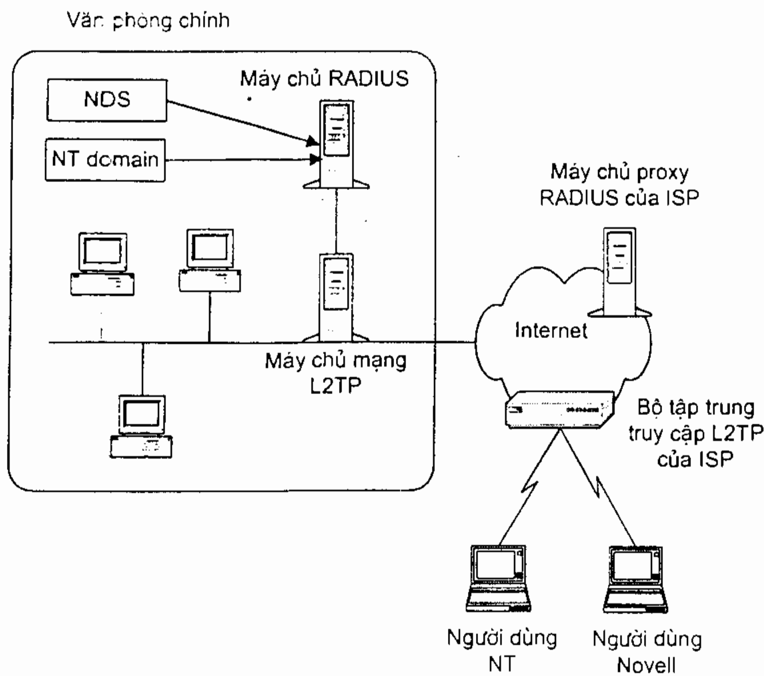
Việc lựa chọn một nhà ISP cung cấp dịch vụ L2TP VPN có thể thay đổi tuỳ theo yêu cầu thiết kế mạng. Nếu thiết kế một VPN đòi hỏi mã hoá đầu cuối-đầu cuối thì cần cài các client tương thích L2TP tại các host từ xa và thoả thuận với ISP là sẽ xử lý mã hoá từ máy đầu xa đến tận máy chủ của mạng VPN. Nếu xây dựng một mạng ít bảo mật hơn, khả năng chịu đựng lỗi cao hơn và chỉ muốn bảo mật dữ liệu khi nó đi trong đường hầm trên Internet thì thoả thuận với ISP để họ hỗ trợ LAC và mã hoá dữ liệu chỉ từ đoạn LAC đến LNS của mạng riêng VPN.

7.2.4 Một ví dụ minh hoạ ứng dụng L2TP trong VPN

Trong ví dụ chỉ đề cập đến việc trao đổi dữ liệu giữa hai điểm cuối, không quan tâm đến thông tin trong mạng được bảo mật như thế nào (sử dụng tường lửa chẳng hạn). Các host được nối tới máy chủ L2TP và mọi ngõ đi ra ngoài đều phải thông qua máy chủ L2TP kết hợp với tường lửa. Kết nối giữa site trong mạng và site bên ngoài phải được khoá lại sao cho chỉ có người quản trị mạng mới truy cập tới được máy chủ mã hoá.

Trong ví dụ hình 7.9, công ty A quyết định sử dụng dịch vụ VPN có hỗ trợ của ISP. Điều này có nghĩa là ISP cung cấp kết nối Internet cho công ty A có máy

chủ proxy RADIUS và LAC. Ở tại công ty A vẫn có duy trì máy chủ RADIUS và LNS. Do ISP có hỗ trợ L2TP nên các máy đầu xa không cần phải cài client L2TP.



Hình 7.9: Quay số L2TP trong VPN

7.3 Khả năng áp dụng của L2TP

L2TP là một thế hệ giao thức quay số truy cập mới của VPN. Nó phối hợp những đặc điểm tốt nhất của PPTP và L2F. Hầu hết các nhà cung cấp sản phẩm PPTP đều đưa ra các sản phẩm tương thích L2TP hoặc sẽ giới thiệu sau này.

Mặc dù L2TP chủ yếu chạy trên mạng IP, nhưng khả năng chạy trên các mạng khác như Frame Relay, ATM đã làm nó thêm phổ biến.

L2TP cho phép một số lượng lớn client từ xa được kết nối vào VPN hay cho các kết nối LAN-LAN có dung lượng lớn. L2TP có cơ chế điều khiển luồng để làm giảm đi tắc nghẽn trên đường hầm L2TP.

L2TP cho phép thiết lập nhiều đường hầm với cùng LAC và LNS. Mỗi đường hầm có thể được gán cho một người dùng xác định, hoặc một nhóm các người dùng và gán cho các môi trường khác nhau tuỳ theo thuộc tính chất lượng dịch vụ QoS của người dùng.

CHƯƠNG 8

THIẾT KẾ VPN

Để thiết kế một VPN hữu dụng, cần phải nắm vững những yêu cầu cho VPN sắp được thiết kế.

Sau đây là một số vấn đề cần liên quan đến xây dựng một site trong VPN:

- Có bao nhiêu người dùng cho mỗi site?
- Loại kết nối đến Internet. Kết nối thường trực hay kết nối theo yêu cầu?
- Lưu lượng mạng do site phát sinh. biến đổi của lưu lượng theo giờ, theo ngày.
- Nếu là kết nối thường trực thì bao lâu kết nối được lưu dự phòng một lần?
- Nếu là kết nối theo yêu cầu thì bao lâu thì được yêu cầu? Độ tin cậy cần thiết phải có?
- Site có hỗ trợ người dùng từ xa không? Nếu có thì bao nhiêu?

Cần phải nắm rõ các loại lưu lượng phát sinh từ site và các loại ứng dụng làm phát sinh các lưu lượng đó. Đối với mạng LAN thì băng thông đủ để đáp ứng cho các loại ứng dụng. Nhưng điều này bây giờ đã thay đổi khi mà World Wide Web ra đời. Lưu lượng bây giờ trở nên lộn xộn và không thể dự đoán trước được. Khi mà các ứng dụng thời gian thực như điện thoại IP, hội nghị truyền hình (video conference),... phát triển thì đặt ra những yêu cầu mới đối với băng thông mạng. Kết nối WAN cũng ảnh hưởng đến việc thiết kế VPN do về kiến trúc thì VPN và WAN đều lớn như nhau. Kết nối WAN truyền thống có băng thông nhỏ hơn kết nối LAN rất nhiều. Do đó cần phải xem xét đến lưu lượng truyền trên kết nối WAN mà có biện pháp nâng cấp băng thông cho phù hợp với lưu lượng đi qua. Băng thông là một vấn đề cần xem xét kỹ khi xây dựng một VPN quay số, bởi vì kết nối giữa ISP và máy chủ tại site VPN cần phải có băng thông đầy đủ để xử lý một số lượng đường hầm đồng thời được tạo ra.

Do VPN được thiết kế không phải chỉ có 2 site liên lạc với nhau mà là tập hợp của rất nhiều site, nên cần phải lưu ý đến vị trí địa lý của các site. Cần phải xem xét đến tính tương tác giữa các site với nhau. Nếu 2 site liên lạc với nhau thường xuyên thì kết nối giữa chúng là kết nối thường trực, còn hiếm khi mới liên lạc với nhau thì chọn kết nối theo yêu cầu. Mặc dù Internet cho phép các site có thể tạo những đường hầm nối thẳng với nhau nhưng nên tổ chức các site theo phân cấp để dễ điều khiển lưu lượng. Vị trí địa lý đóng vai trò quan trọng đối với việc bảo mật. Nếu một mạng VPN phủ trên nhiều quốc gia thì không chắc giải thuật mã hoá và chiều dài từ khoá ở nơi này lại được chính phủ nơi khác chấp nhận. Chính phủ Mỹ có thể thay đổi quan điểm của họ về việc xuất khẩu chiều dài từ khoá. Một số sản phẩm VPN phải được công nhận bản quyền từ phía Hoa Kỳ. Trong tình hình này phải xây dựng hệ thống hỗ trợ ít nhất là 2 chiều dài từ khoá khác nhau.

Tính hợp thời của dữ liệu cũng là một yếu tố cần quan tâm khi xây dựng một VPN thương mại. Một dữ liệu thương mại đã cũ 2 năm thì không thể được xử lý như một dữ liệu mới 2 tuần. Khi mà nắm vững chu kỳ dữ liệu cần bảo mật thì sẽ chọn được chiều dài từ khoá và giải thuật mã hoá hợp lý để bảo mật dữ liệu đó.

Khả năng mở rộng VPN thành Extranet cần được quan tâm. Nếu như Extranet là một phần trong kế hoạch phát triển mạng thì cần quan tâm đến khả năng của mạng hiện tại và các ứng dụng được sử dụng trong tương lai. Sau đây ta khảo sát một số vấn đề về thiết kế.

8.1 Các vấn đề về mạng

Một trong những vấn đề về mạng cần phải quan tâm đó là các thiết bị định tuyến và bảo mật. Có thể thêm phần cứng hoặc phần mềm vào bộ định tuyến để nó đóng vai trò là một cổng nối bảo mật trong VPN. Tuy nhiên, nếu như bộ định tuyến và tường lửa đã cố gắng tối đa nhưng vẫn không thay thế được các chức năng của VPN thì có 3 cách chọn lựa:

- Nâng cấp bộ định tuyến hoặc tường lửa lên để hỗ trợ các chức năng của VPN.
- Thay thế bộ định tuyến hay tường lửa bằng thiết bị thuộc thế hệ mới, tương thích hơn.
- Sử dụng thiết bị khác để cung cấp dịch vụ VPN.

Mã hoá là một tiến trình đòi hỏi tính toán, tuy nhiên nó thay đổi tuỳ theo giải thuật. Một số nhà cung cấp đã đưa ra một số card đồng xử lý mã hoá cho bộ định tuyến và tường lửa để giúp thêm khả năng mà VPN cần.

Một thiết bị cần quan tâm khi nâng cấp từ một mạng hiện có lên VPN là máy chủ truy cập từ xa RAS (Remote Access Server). Một trong những nỗ lực của

VPN là cố gắng chuyển việc quản lý, hỗ trợ và thiết bị được yêu cầu từ mạng riêng sang ISP. Khi xây dựng một VPN thì vẫn có thể duy trì RAS cũ và dựa thêm vào hỗ trợ của ISP để cho RAS tương thích với VPN.

Một thành phần vẫn còn có thể sử dụng lại được trong VPN là hệ thống xác thực cho người dùng từ xa. Nhiều thiết bị VPN có thể sử dụng được hệ thống xác thực cho người dùng từ xa như TACACS+, xác thực dựa trên thẻ bài. Việc tương thích này cho phép tiếp tục duy trì hệ thống xác thực khi chuyển từ mạng truy cập từ xa RAN (Remote Access Network) lên VPN.

Hai vấn đề quan trọng cần phải giải quyết là định tuyến và phân giải tên. Có hai hướng để giải quyết vấn đề này. Hướng thứ nhất: xem mạng như một mạng đơn bao trùm lấy toàn bộ các site. Hướng thứ hai là xem mỗi site như một phần mạng riêng và các site được nối kết với nhau thông qua đường hầm.

Có thể áp dụng định tuyến đầy đủ (full routing) giữa các phần của mạng kết nối bởi đường hầm và dùng tên thống nhất cho DNS. Một công ty không thể đăng ký được một mảng địa chỉ IP thực rộng lớn do tài nguyên địa chỉ IP đang dần bị cạn kiệt. Có thể dùng giải pháp gán địa chỉ IP nội bộ cho các host trong mạng và sử dụng dịch địa chỉ mạng NAT để chuyển đổi chúng thành các địa chỉ IP thực được cấp (hình 8.5). Điều này có thể làm nảy sinh vấn đề đối với VPN khi mà 2 site cố gắng kết nối với nhau thông qua đường hầm thì có thể có trường hợp 2 địa chỉ mạng trùng nhau, sẽ làm phá vỡ việc định tuyến và một số chức năng khác của mạng.

Một vấn đề nữa là khi xây dựng VPN cần quan tâm đến vấn đề nâng cấp mạng lên IPv6 trong tương lai. Mặc dù IPv6 đang phát triển chậm nhưng cần chọn giao thức có thể hỗ trợ IPv6 (IPSec) để có thể dễ dàng nâng cấp mạng trong tương lai.

8.2 Các vấn đề về bảo mật

Quyền truy cập là vấn đề cần quan tâm khi xem xét tới việc bảo mật cho VPN.

Bởi vì VPN có thể cho phép người dùng truy cập tới những mạng con hoặc thiết bị nhưng cũng có thể cấm truy cập tới những phần khác của mạng.Tổng quát thì một đường hầm có thể cho phép người dùng truy cập vào mạng mà không có sự ngăn cấm nào. Tuỳ theo giao thức sử dụng và hệ điều hành mạng mà có thể chỉ định cho quyền truy cập đường hầm khi mà đường hầm được thiết lập.

Khi muốn kiểm soát lưu lượng trên mạng thì cần thiết kế VPN sao cho mọi lưu lượng đến phải thông qua tường lửa trước khi đến được mạng bên trong.

Một giải pháp phổ biến cho công ty khi muốn chia sẻ một phần thông tin từ VPN của mình cho người dùng Internet hay khách hàng của họ trong khi vẫn bảo mật được tài nguyên riêng của họ đó là sử dụng vùng giới tuyến DMZ

(Demilitarized Zone) như trong hình 8.6. DMZ bao gồm có 2 tường lửa: một đặt giữa Internet mà tài nguyên muốn chia sẻ, một đặt giữa tài nguyên chia sẻ và mạng nội bộ bên trong. Máy chủ trong DMZ đóng vai trò như nơi lưu trữ thông tin phụ sao cho nếu như nó bị hư hỏng thì chỉ có một ít thiệt hại xảy ra. Ví dụ như máy chủ Web trong DMZ lưu những bản sao trang web còn bản chính thì nằm trên máy chủ ở trong mạng nội bộ.

Hai thành phần của bảo mật được xem là mới khi giới thiệu trong VPN đó là chuyển giao khoá (key exchange) và chứng nhận số (digital certificate)

Khi thiết kế VPN cần quyết định bao lâu thì khoá được chuyển một lần giữa các cổng nối bảo mật. Nếu VPN chỉ có một số lượng nhỏ cổng nối bảo mật thì chuyển khoá bằng tay vẫn là một giải pháp có thể chấp nhận được. Tuy nhiên nó sẽ không khả thi khi VPN trải rộng trên cả một quốc gia hay khắp toàn cầu. Trong trường hợp như vậy phải sử dụng đến e-mail bảo mật hoặc gửi bưu phẩm bảo đảm.

Để đảm bảo bảo mật cho dữ liệu cao nhất thì tốt hơn hết là sử dụng hệ thống chuyển khoá tự động. Những khoá sử dụng cho mã hoá và xác thực có thể tự động thay đổi theo những qui luật sau: sau một số lượng gói được truyền đi, sau một khoảng thời gian, mỗi khi bắt đầu một phiên làm việc mới hoặc là tổ hợp của những qui luật trên. Tự động thay đổi khoá làm tăng khả năng chống lại các vụ tấn công.

Khi chọn một hệ thống quản lý khoá thì cần kèm theo một số cơ chế phục hồi khoá. Điều này đặc biệt hữu ích khi muốn khôi phục lại dữ liệu cũ dùng với khoá cũ trước đó.

Trong tiến trình mã hoá khoá chung có sử dụng một cặp khoá chung để xác thực tính hợp lệ của khoá. Việc xác thực tính hợp lệ này gọi là chứng nhận số. Những chứng nhận này nhằm ràng buộc khoá chung với một thực thể được mang tên, có thể là người dùng hay máy tính. Nhiều trình duyệt Web sử dụng chứng nhận điện tử để bảo đảm truyền thông bảo mật với máy chủ sử dụng Secure Sockets Layer cho các mục đích thương mại điện tử. Một số hệ thống e-mail đưa ra khả năng mã hoá dựa trên chứng nhận điện tử và những công nghệ được sử dụng để phân phối chúng: chứng nhận điện tử CA và cơ sở hạ tầng khoá công cộng PKI (Public Key Infrastructures).

8.3 Các vấn đề về ISP

ISP có liên quan đến VPN theo nhiều hướng. Sử dụng PPTP và L2TP cho đường hầm cho phép ISP đưa ra nhiều dịch vụ gia tăng giá trị như bộ khởi tạo đường hầm và proxy hỗ trợ cho xác thực của VPN. Mặc khác, ISP cũng cung cấp đầy đủ nguồn xuất VPN.

Cần lưu ý là ISP đang cung cấp không phải là nhà cung cấp VPN duy nhất. Có thể sử dụng nhiều ISP cho VPN. Một lý do để sử dụng nhiều ISP là phạm vi địa lý rộng lớn của mạng VPN.

Nếu như có kế hoạch sử dụng PPTP hay L2TP để xây dựng VPN thì cần xem xét đến khả năng của thiết bị của ISP và họ xử lý vấn đề bảo mật như thế nào. Nếu một ISP dùng máy chủ Proxy RADIUS thì cần phải đảm bảo việc bảo mật chống lại truy cập của những khách hàng của ISP đó hoặc ngay các nhân viên đang làm việc tại ISP.

Tốt hơn hết là nên có một máy chủ RADIUS ngay tại VPN cho việc xác thực người dùng và cho phép máy chủ Proxy của ISP làm việc dựa trên những dữ liệu do máy chủ đó cung cấp.

PHẦN II

XÂY DỰNG CÁC KHỐI CỦA MỘT VPN

Một VPN bao gồm hai thành phần chính: tuyến kết nối đến Internet do một nhà cung cấp dịch vụ Internet - ISP (Internet Service Provider) cung cấp và phần mềm cũng như phần cứng để bảo mật dữ liệu bằng cách mã hoá chúng trước khi truyền chúng ra Internet (do Internet là một mạng công cộng không có tính bảo mật). Các chức năng của VPN có thể được thực hiện bằng các bộ định tuyến, tường lửa và những phần cứng được thiết kế đặc biệt làm cho việc triển khai các thiết bị của VPN trở nên dễ dàng hơn.

Do VPN có vai trò quan trọng trong việc kinh doanh của chúng ta nên ta phải bảo đảm mạng của mình đạt hiệu suất cao nhất có thể mà ISP cung cấp thông qua một hợp đồng cung cấp dịch vụ đã được thỏa thuận trước SLA (Service Level Agreement). SLA được định nghĩa qua thông lượng mong đợi và độ trì hoãn tối đa có thể chấp nhận, chúng ta cần kế hoạch sao cho công ty có thể giám sát được chất lượng mạng để đảm bảo tính hoạt động trôi chảy của mạng. Tuy nhiên, khi chọn các thiết bị để thực hiện mã hoá và định đường hầm cho VPN của mình, chúng ta sẽ phải cân nhắc giữa thông lượng WAN mong đợi với khả năng của thiết bị sao cho phù hợp.

Trong phần 2 này, chúng ta sẽ đề cập đến những vấn đề liên quan đến việc tạo ra một VPN như việc kết nối đến ISP, việc sử dụng bộ định tuyến và tường lửa trong VPN, trình bày về thiết bị phần cứng, sản phẩm phần mềm cần thiết cho VPN thông dụng hiện nay và các yêu cầu chung về chúng.

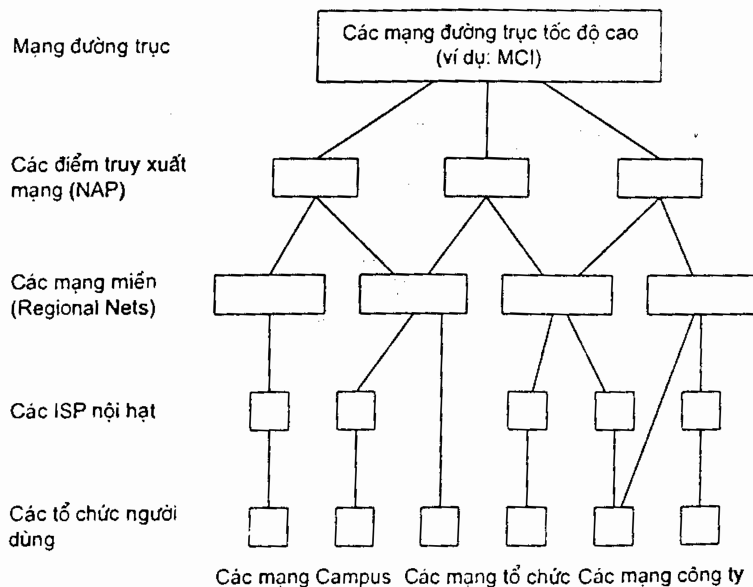
CHƯƠNG 9

KẾT NỐI CỦA ISP

Tuyến kết nối do ISP cung cấp là một yếu tố rất quan trọng trong việc xây dựng nên một VPN bởi vì ISP đóng vai trò là người chịu trách nhiệm về đường truyền dữ liệu, duy trì kết nối cho chúng ta hoạt động thông qua mạng Internet. Do đó trong phần này ta sẽ đề cập đến những khía cạnh liên quan đến ISP như khả năng của ISP, phân loại các ISP, các hợp đồng SLA ...

9.1 Khả năng của một ISP

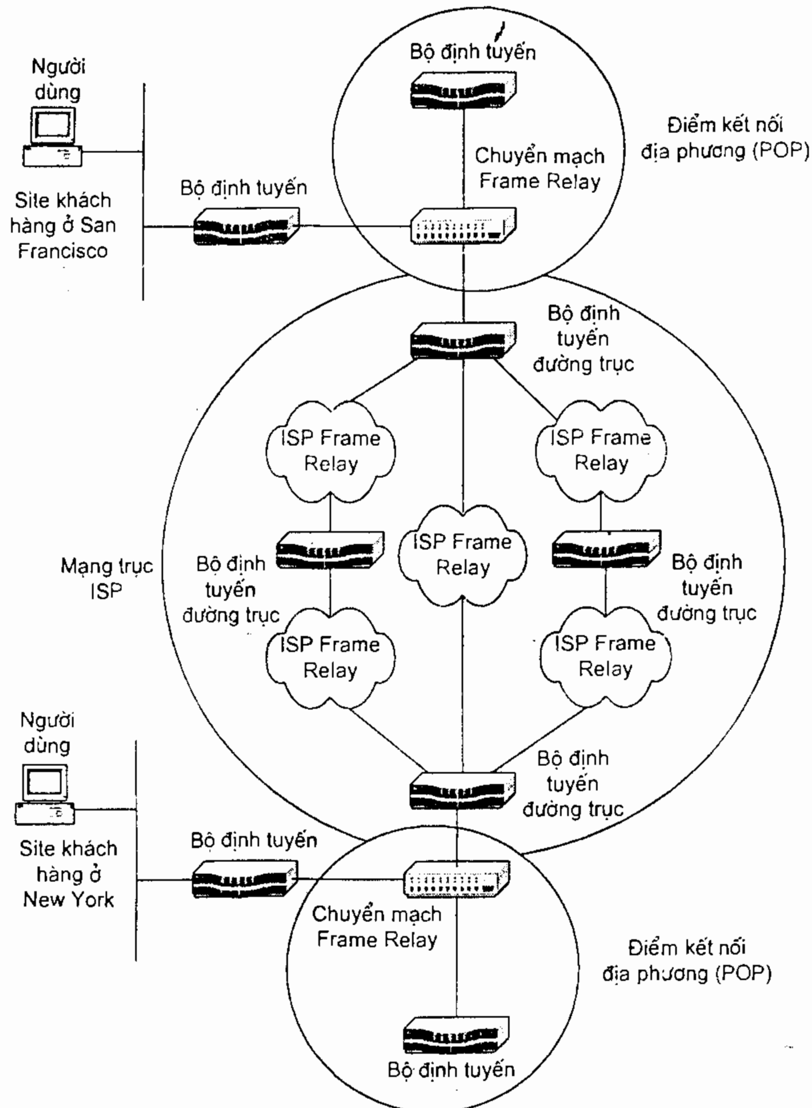
Trước khi thảo luận về những dịch vụ mà ISP có thể cung cấp, chúng ta hãy xem xét việc phân lớp các ISP theo khả năng cũng như kiến trúc mạng của họ kèm với cấu trúc Internet.



Hình 9.1: Kiến trúc của những nhà cung cấp dịch vụ Internet

9.1.1 Các dạng ISP

Các nhà cung cấp mà mạng của họ là một thành phần trong mạng Internet có thể được chia theo bậc thang tùy vào khả năng, quy mô mạng và dạng kết nối đến Internet của các ISP này. Theo cách chia dựa vào những quy tắc trên, người ta có thể chia ISP ra làm các nhóm sau: (xem hình 9.1).



Hình 9.2: Một mạng đường trục ISP tiêu biểu

- Nhóm 1: nhóm các nhà cung cấp mạng chính và các mạng riêng ảo của họ đóng vai trò là mạng đường trục (backbone) cho Internet (do mạng có tốc độ cao, tin cậy ...), các ISP thuộc nhóm này thường là những quốc gia phát triển cao, có mạng lưới thông tin mạnh (Mỹ, Anh, Singapore, Nhật ...), hoặc là những công ty

đa quốc gia có thể kể đến như AT&T, IBM, UUNET, PSInet.... Các ISP này thường có kiến trúc mạng tiêu biểu như hình dưới (xem hình 9.2)

Các mạng này độc lập và kết nối với nhau thông qua những điểm truy cập mạng NAP (Network Access Points), hay nói cách khác, các mạng này đấu nối với nhau và chuyển giao lưu lượng tại các NAP để tạo ra những yếu tố cần thiết cho việc hoạt động của Internet. Các mạng quốc gia tạo ra một cách độc lập bởi các công ty như UUNET, PSInet và một số công ty khác thường được đấu nối vào các NAP. Một số nhà cung cấp tự thu xếp việc chuyển giao lưu lượng Internet không qua các NAP để tránh hiện tượng nghẽn mạch, những điểm ngang cấp nhau (peering points) giúp thay phiên nhau trong việc tải lưu lượng lên các NAP.

Lưu ý các không có NAP nào cung cấp các kết nối đến Internet từ một trong những nhà cung cấp nhóm một này đến mạng công cộng hay tới các doanh nghiệp. Các NAP chỉ là những điểm nhằm chuyển giao lưu lượng giữa các tổ chức cùng bảo dưỡng các mạng đường trục quốc gia rộng lớn mà thôi. Một NAP không phải là một điểm với mục đích chỉ để truy cập đến Internet. Về tốc độ, các kết nối đến các NAP Internet này phải được tạo ra với tốc độ tối thiểu là tốc độ DS-3 (45Mbit/s).

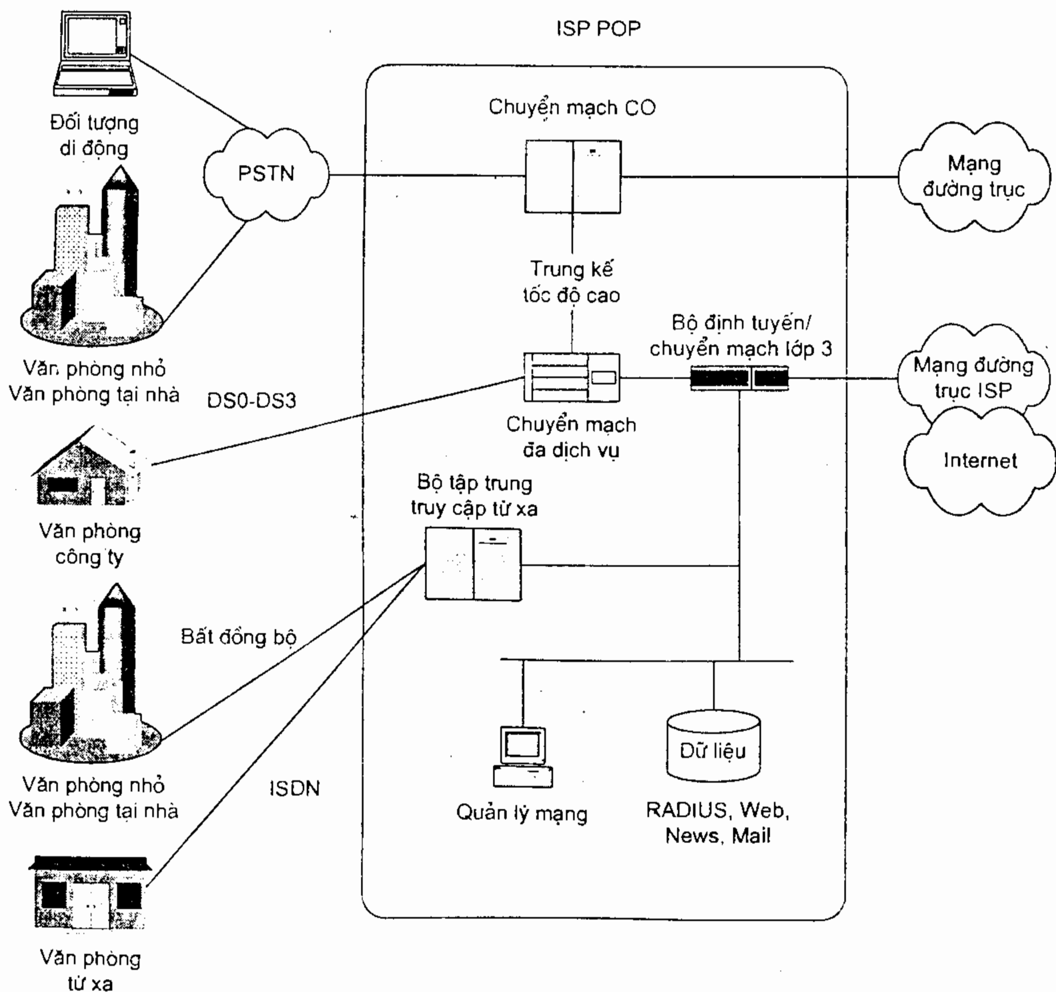
- Nhóm 2: là những công ty mua những kết nối đến Internet từ một trong những nhà cung cấp nhóm một ở trên, rồi sau đó họ cung cấp lại cho khách hàng dưới các dạng quay số thường trực, cho khách hàng thuê các địa chỉ trang Web, hay bán lại băng thông. Những nhà cung cấp địa phương tiêu biểu hoạt động ở các mạng đường trục trong giới hạn một hay nhiều các trạng thái liên tiếp nhau. Ngoài ra, họ cũng có thể kết nối đến NAP, nhưng thông thường là không quá một NAP.

- Nhóm 3: Là nhóm các ISP hoạt động bên dưới các ISP của nhóm 2, đây là những ISP độc lập, có thể ở quy mô nhỏ như chỉ có từ 2 hay 3 khách hàng sử dụng bằng cách quay số vào các điểm kết nối ở địa phương POP (Point of Presence) cho đến quy mô lớn hỗ trợ hàng trăm ngàn khách hàng quay số. Những nhà cung cấp này thông thường không nắm quyền điều khiển mạng đường trục hay thậm chí là mạng quốc gia của họ. Nếu họ thực hiện dịch vụ quốc gia, họ sẽ sử dụng các POP và cấu trúc mạng đường trục của một nhà điều hành lớn hơn mà họ liên kết đến.

Đối với một doanh nghiệp thường xuyên phải liên kết đến Internet hoặc một người độc lập làm việc tại nhà thì các POP này có vị trí quan trọng trong việc sử dụng Internet. POP là nơi mà ISP điều khiển các môi trường làm việc khác nhau và cũng là nơi ISP chuyển các lưu lượng của các khách hàng đến mạng đường trục của Internet, nhằm kết nối đến một số điểm thuộc phần còn lại của Internet (xem hình 9.3).

Một vài POP bao gồm những thiết bị khác nhau dành cho mỗi môi trường truyền dẫn như các nhóm modem cho các phiên quay số và các CSU/DSU dành cho công nghệ Frame Relay và những dịch vụ dữ liệu số (Digital Data Service), một số ISP đã chọn việc từ bỏ việc hỗ trợ cho các môi trường khác nhau để dùng mạng công cộng, thay cho việc dùng một kênh thuê riêng đến các POP của họ (nhằm giảm bớt chi phí kết nối). Ngoài ra, để điều khiển các môi trường khác nhau cho lưu lượng của khách hàng, POP còn bao gồm các bộ định tuyến/chuyển mạch để kết nối mạng LAN cục bộ của POP đó đến các mạng khác của ISP như các thiết bị mở rộng để quản lý mạng.

Dịch vụ cơ bản nhất của một ISP là tuyến kết nối đến Internet mà họ cung cấp, tuyến kết nối này có thể ở dạng đơn giản nhất như việc cung cấp cho những khách hàng việc truy cập quay số bằng modem hay đường ISDN, hoặc nó có thể là một đường T1 hay T3 nối từ LAN của công ty đến điểm truy cập địa phương (POP) của ISP và sau đó đến Internet.



Hình 9.3: Sơ đồ một ISP POP điển hình

9.1.2 Cơ sở hạ tầng của ISP

Mối quan tâm đầu tiên của chúng ta là mạng đường trục của ISP, bởi vì nó xác định lưu lượng của mạng được điều khiển tốt hay không và mức độ như thế nào. Cách thiết kế tốt nhất là tạo một mạng lưới đầy đủ các đường dẫn vòng chuyển tiếp giữa các điểm truyền dẫn. Các bộ định tuyến/chuyển mạch dự phòng cũng có thể được cài đặt tại mỗi điểm truyền dẫn chính trên mạng. Mỗi vị trí bộ định tuyến hay chuyển mạch trên mạng sẽ được đấu nối tại trung tâm dữ liệu để điều khiển môi trường, còn bao gồm các phần tử khác như nguồn điện dự phòng.

Mặc dù với trạng thái hiện tại của Internet cho phép ta nhận được các dịch vụ VPN tốt nhất từ nhà cung cấp thông qua những mạng quốc gia và mạng quốc tế của họ, chúng ta cũng có thể tạo ra những VPN để điều khiển các lưu lượng chuyển qua ranh giới ISP như các VPN quay số đến Internet. Hơn nữa, chúng ta có thể cần phải điều độ cân bằng giữa lưu lượng của VPN với lưu lượng không bảo mật khác liên quan đến việc kinh doanh của mình trong cùng một ISP.

9.1.3 Các tùy chọn của kết nối

Đa số các ISP nổi tiếng trong các dịch vụ kinh doanh thường bán đầy đủ các tùy chọn cho kết nối với các sản phẩm hỗ trợ băng thông từ 56 kbit/s đến tốc độ T3 đang ngày càng trở nên phổ biến. Khi lập kế hoạch cho một kết nối dùng băng thông riêng, ta phải xác định kết nối đó thực sự không bị ai đó can thiệp vào. Ví dụ, một số ISP hỗ trợ một đường T1 trong dạng thức của Ethernet, làm cho việc tích hợp mạng trở nên dễ dàng hơn, vì mạng cục bộ (LAN) ngày nay thường là các Ethernet hay Fast Ethernet (tốc độ 100Mbit/s). Một số ISP khác lại cung cấp tuyến T1 trong dạng thức một tuyến thô (raw serial), nên ta phải cần dùng cổng nối để chuyển dạng nó thành một giao thức mà chúng ta có thể sử dụng.

Một số ISP yêu cầu chúng ta phải mua các thiết bị như bộ định tuyến và các CSU/DSU, trong khi một số ISP khác sẽ hỗ trợ và quản lý chúng cho ta, điều này có tính thuận lợi hơn cho các công ty muốn thu hồi vốn nhanh, ít chi phí. Thông thường các ISP sẽ hỗ trợ chúng ta trong việc cấu hình, giám sát, chẩn đoán các lỗi thông qua trung tâm điều hành mạng NOC (Network Operation Center) của họ. Một điều rất thuận lợi cho chúng ta là trung tâm điều hành mạng này hoạt động thường xuyên 24/24 trong suốt 7 ngày mỗi tuần và đội ngũ nhân viên rất lành nghề, sẵn sàng phục vụ khách hàng của họ.

Đa số các ISP đều có 3 loại cước trong các dịch vụ truy cập mạng của họ, đó là: cước cài đặt, cước dựa trên loại dịch vụ băng thông của kết nối mà bạn đăng ký (cước dịch vụ) và cước truy cập mỗi khi chúng ta truy cập đến điểm truy cập mạng địa phương của ISP (POP).

9.2 Các hợp đồng lớp dịch vụ SLA

Ngay khi chúng ta vạch ra kế hoạch cho việc triển khai những dịch vụ cho VPN của mình thì một số vấn đề mà chúng ta cần phải quan tâm đến như hiệu suất mạng, việc bảo dưỡng và cách khắc phục sự cố. Và một phương án nhằm để đảm bảo những yêu cầu trên được nhà cung cấp dịch vụ đáp ứng nghiêm túc đó là việc nhà cung cấp phải cho chúng ta một hợp đồng về tính chất, đặc điểm, chất lượng dịch vụ họ cung cấp, hợp đồng này còn gọi là hợp đồng lớp dịch vụ hay gọi tắt là SLA.

Các hợp đồng SLA là những thỏa thuận trên văn bản về lớp dịch vụ mà khách hàng đăng ký với ISP, chúng có một mục đích chính là hạn chế tranh giành về quyền lợi giữa ISP và khách hàng, sao cho hai bên đều cảm thấy vừa ý với lợi ích mà mình được hưởng, bằng cách thiết lập những lý do mong đợi hợp lý về dịch vụ, SLA giúp ích cho cả doanh nghiệp và khách hàng bằng cách cung cấp tiêu chuẩn có hiệu lực và bảo mật quyền lợi cho họ ngay cả ở những dịch vụ khiêm tốn nhất. SLA cũng có ích cho ISP bằng việc cung cấp một cách để đảm bảo những khả năng mà ISP đã thiết lập là đúng và giúp họ phán đoán được lỗi.

Mọi SLA đều có ba phần tử chính mà chúng ta không thể không đề cập đến, đó là:

- Độ sẵn sàng;
- Thông lượng thật sự (thông lượng hiệu dụng);
- Độ trễ.

Ngoài ra, đôi khi người ta còn đề cập đến các phần tử khác như thời gian không xảy ra lỗi, thời gian sửa chữa hay phục hồi dịch vụ.

Độ sẵn sàng của mạng là tiêu chuẩn đơn giản để đánh giá về thời gian mà mạng sẵn sàng phục vụ khách hàng, ta có thể tham khảo một công thức tính độ sẵn sàng của mạng trong tháng như sau:

$$\frac{\text{(24 giờ x số ngày của tháng x số vị trí) - thời gian mạng ngưng hoạt động}}{\text{(24 giờ x số ngày của tháng x số vị trí)}}$$

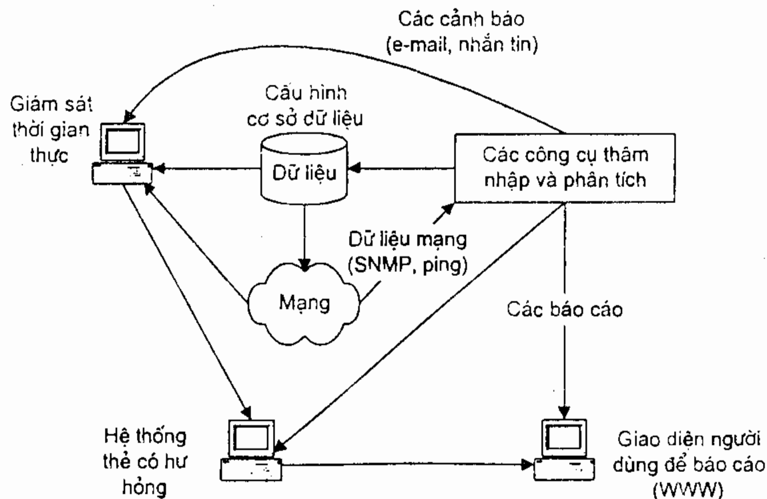
Các bước để chuẩn bị cho một SLA

1. Luôn xác định các mức độ dịch vụ nào ở WAN là cần thiết.
2. Luôn kiểm tra mỗi khi thực hiện các cấp dịch vụ, cần giám sát hiệu suất mạng ở trạng thái hiện tại cũng như xem lại hiệu suất trong quá khứ và đánh giá bất kỳ xu hướng nào làm ảnh hưởng đến chất lượng mà ta nhận thấy được.
3. Định ranh giới mạng, tìm hiểu các ứng dụng trên mạng, thời gian cao điểm và các vùng có thể bị tắc nghẽn.

4. Thương lượng về SLA mọi lúc nếu có thể. Đọc kỹ tài liệu và thực hiện những tính toán cần thiết. Nếu như ta đã có một thỏa thuận về độ sẵn sàng của mạng là 99.5%, thì xem thử trong một tháng có bao nhiêu giờ mạng không đáp ứng được?
5. Trình bày rõ ràng về dự án cho việc giám sát nhà cung cấp của mình.
6. Phân tích hiệu suất mạng và độ tin cậy mỗi tuần một lần.
7. Hàng tháng phải so sánh những tiêu chuẩn của chúng ta về những đặc tính mạng với các bản báo cáo của nhà cung cấp.

Giám sát hiệu suất của ISP

Mỗi khi chấp nhận một SLA chuẩn cung cấp bởi ISP hay dành thời gian cho việc thực hiện SLA của mình, thì mỗi SLA sẽ không đầy đủ nếu thiếu một số yếu tố trong việc giám sát cấp độ dịch vụ đã được chỉ ra trong SLA



Hình 9.4: Giám sát và quản lý mạng

Một hệ thống quản lý mạng có nhiều thành phần, như trong hình 9.4 đã trình bày, nhưng có 4 yếu tố quan trọng nhất đối với việc giám sát hiệu suất của nhà cung cấp là:

1. Các thiết bị giám sát đặt tại ranh giới với mạng của nhà cung cấp.
2. Một cơ sở dữ liệu để thu thập thông tin về hiệu suất.
3. Các ứng dụng được thiết kế để phân tích dữ liệu và phát hành các bản báo cáo cho mỗi khách hàng trong mạng.
4. Các bản báo cáo ở dạng Web để khách hàng dễ đọc, dễ hiểu (tận dụng những ưu điểm của Web như việc tích hợp âm thanh, hình ảnh, video vào cùng một siêu văn bản).

9.3 Nhận xét đánh giá về ISP

ISP đóng vai trò quan trọng trong việc thiết kế và hoàn thành VPN của chúng ta, việc thiết kế VPN sẽ chỉ ra những liên quan đến ISP của ta và có thể giới hạn vai trò của ISP như chỉ cung cấp đường dẫn cho mạng VPN đến Internet, hoặc có thể tận dụng ISP như một nhà thiết kế hay bảo dưỡng một VPN.

Khi đánh giá một ISP cho mạng VPN của mình, chúng ta phải bàn tính đến nhiều chi tiết khác nhau, nhưng thông thường có thể liệt kê một số chi tiết như sau: cơ sở hạ tầng của ISP, hiệu suất và quản lý mạng, các tùy chọn cho một kết nối và cả vấn đề bảo mật.

Khi dự định thiết lập một mối quan hệ giữa công ty và một ISP, chúng ta nên xem xét kỹ về việc bản hợp đồng cấp dịch vụ SLA giữa ta và ISP để thiết lập những khả năng đối với hiệu suất mạng và cách giải quyết của ISP khi có sự cố, việc sửa chữa mạng và những vấn đề khác liên quan của ISP có tốt hay không. Nếu chúng ta sử dụng SLA, nên xem xét hiệu suất mạng của ISP song song với những hệ thống đo lường của ISP để đảm bảo các chỉ định trong SLA là phù hợp

Cuối cùng, nếu ta muốn mở rộng giao tiếp mạng (outsource) VPN của mình đến một nhà cung cấp, thì ta nên liên hệ một số các nhà cung cấp lớn họ có thể giúp đỡ chúng ta thực hiện mong muốn trên. Ta có thể tham khảo một số nhà cung cấp như: AT&T, ANS, WorldNet, InternetMCI, UUNET ...

CHƯƠNG 10

TƯỜNG LỬA VÀ BỘ ĐỊNH TUYẾN

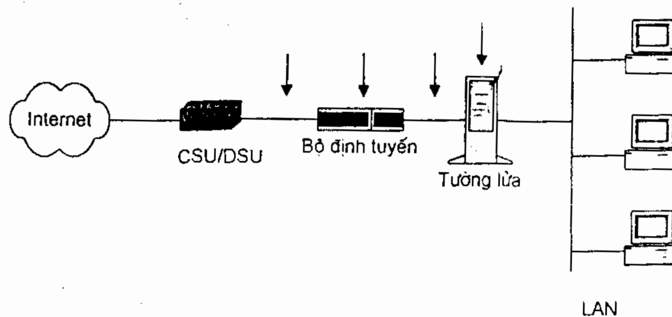
Sau khi đã có một kết nối đến Internet, thì trong mạng VPN của chúng ta còn phải cần đến một số thiết bị không kém phần quan trọng khác để điều khiển truy cập đến mạng LAN cần được bảo mật của mình, tức là chống lại những xâm nhập bất hợp pháp. Các thiết bị đó là các cổng nối bảo mật mà trong phần này chúng ta sẽ đề cập nhiều về chúng. Các nhân viên di động vẫn có thể truy cập đến Internet thông qua máy tính xách tay của mình bằng cách sử dụng một kênh do một ISP cung cấp, hoặc những khách hàng cũng có thể định đường hầm (tunneling) đến mạng LAN của công ty chúng ta thông qua mạng Internet. Lý tưởng hơn là các thiết bị VPN có thể điều khiển các tình huống này rất tốt.

Do mỗi ISP lại có một đề xuất riêng của họ về những thiết bị cho VPN, cho nên việc phân loại cho các sản phẩm phần mềm và phần cứng cho VPN gặp rất nhiều khó khăn. Trong phần này và những phần kế, chúng ta sẽ đề cập đến những thông tin hữu ích để xác định chúng ta sẽ chọn các giải pháp tách rời (theo mô đun) hay là giải pháp tích hợp.

Phần cứng và phần mềm của một VPN có thể đặt tại những nơi khác nhau trên mạng. Ta sẽ dành ra một ít thời gian để xem xét bằng cách nào mà một nơi trong mạng VPN có thể kết nối đến Internet thông qua một ISP (xem hình 10.1).

Tại đầu tuyến đến từ POP của ISP, chúng ta sẽ có một thiết bị CSU/DSU sau đó là một bộ định tuyến, một tường lửa và một LAN của công ty. Các thiết bị VPN có thể đặt tại những nơi khác nhau trong suốt tuyến kết nối từ LAN này cho đến ISP kia. Nhắc lại rằng một ISP thực sự mạnh hay không thì còn tùy thuộc vào mã hoá, xác thực và các dịch vụ định đường hầm. Các thiết bị hỗ trợ những dịch vụ trên có thể được đặt giữa CSU/DSU và bộ định tuyến hoặc giữa bộ định tuyến với tường lửa. Những sản phẩm khác cung cấp những dịch vụ cho VPN thì xem như đó là một phần của tường lửa hoặc bộ định tuyến. Một vài sản phẩm tích hợp

toàn bộ những dịch vụ mạng giữa ISP và LAN sẽ gom toàn bộ những liên kết WAN, định tuyến, các tường lửa và những dịch vụ cho VPN thành một sản phẩm duy nhất. Sau cùng, một vài hệ điều hành mạng như Windows NT và Novell Netware tích hợp luôn những hỗ trợ cho VPN.



Hình 10.1: Vị trí các thành phần trong VPN

Chúng ta sẽ bắt đầu xem xét việc sử dụng những tường lửa hoặc những bộ định tuyến trong việc xây dựng một VPN. Sau đó ở phần kế tiếp ta sẽ dành một ít thời gian để xem xét về yếu tố phần cứng trong VPN bao gồm những thiết bị mã hoá chạy độc lập hay những thiết bị tích hợp.

10.1 Tường lửa

10.1.1 Một vài điểm quan trọng ở các tường lửa

Từ lâu, các tường lửa đã được sử dụng cho việc bảo mật mạng WAN khỏi tấn công của những kẻ phá hoại (attacker/hacker) trong khi đấu nối liên mạng bằng cách điều khiển quyền truy cập đến những tài nguyên chủ yếu dựa trên các dạng gói, loại ứng dụng và địa chỉ IP. Gần đây, việc triển khai các tường lửa phát triển một cách nhanh chóng do mạng Internet ngày càng thu hút các doanh nghiệp trong việc kinh doanh trên mạng, do đó càng ngày càng có nhiều doanh nghiệp muốn đấu nối mạng của họ với Internet. Nếu mạng của chúng ta được kết nối vào Internet, ta phải sẵn sàng cho việc triển khai ít nhất một tường lửa để điều khiển lưu lượng đến từ Internet.

Các tường lửa và những chính sách bảo mật

Một tường lửa là một phần tích hợp trong chính sách bảo mật của tổ chức chúng ta, bởi vì nó xác định lưu lượng chuyển qua giữa mạng Intranet của ta với mạng Internet (tường lửa còn có thể dùng để bảo mật những vùng giới hạn thâm nhập đối với các vùng còn lại trong mạng của mình: tức là một số vùng không phải người dùng nào cũng có thể đăng nhập vào đó). Ngoài ra, trong chính sách

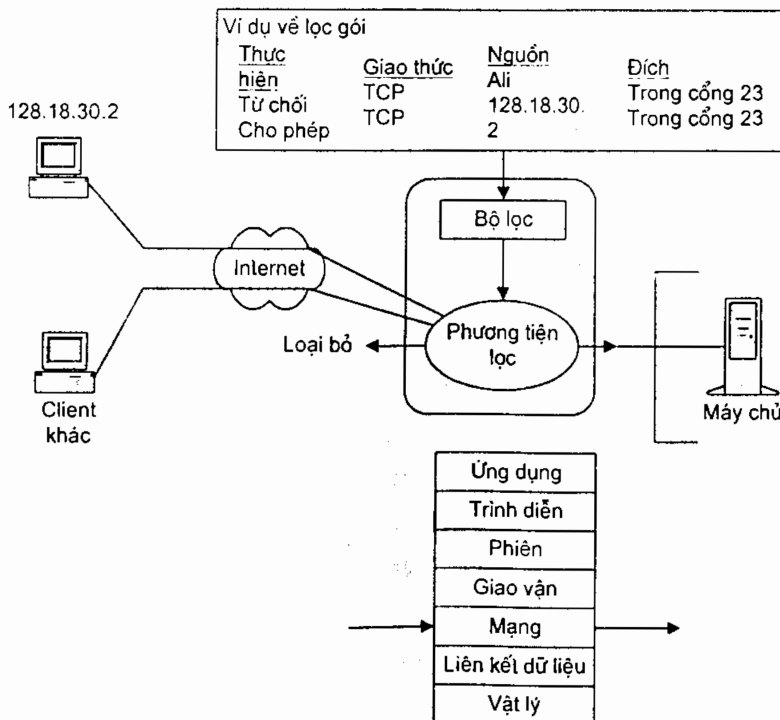
bảo mật của công ty có thể kèm theo việc sử dụng mật khẩu đối với các hệ thống cần được bảo mật nghiêm ngặt, việc mã hoá dữ liệu, sao lưu dữ liệu và quản trị tài khoản đăng ký (account) của người dùng. Ví dụ như đối với một ISP, việc bảo mật tên người dùng và mật khẩu cho các khách hàng của mình là một việc cực kỳ quan trọng, cần được mã hoá và bảo mật nghiêm ngặt.

Sau đây ta sẽ đề cập đến các loại tường lửa thường gặp: các bộ lọc gói (Packet Filters), các proxy kênh (Circuit Proxies), các proxy ứng dụng (Application Proxies) và những tường lửa sử dụng những bộ lọc gói thông minh (Smart packet Filters)

10.1.2 Các loại tường lửa

Các bộ lọc gói

Các tường lửa sử dụng lọc gói là những tường lửa xuất hiện sớm nhất. Các bộ lọc gói sẽ dò địa chỉ nguồn và địa chỉ đích của tất cả các gói IP đến để cấm hay cho phép chuyển các gói này đi qua tường lửa dựa trên những quyền mà người quản trị mạng đã thiết lập (xem hình 10.2).



Hình 10.2: Lọc gói

Hai lợi điểm của các tường lửa lọc gói là chúng dễ thực hiện hơn các loại tường lửa khác và thứ hai là hoạt động mạng tính trong suốt đối với các người dùng đầu cuối (ở phần sau chúng ta sẽ thấy các loại tường lửa khác không có tính

trong suốt này). Tuy nhiên, trong thực tế chúng cũng gây một số khó khăn cho chúng ta trong lúc cấu hình tường lửa sao cho đúng, đặc biệt là khi cần phải tạo nhiều quyền (rules) để điều khiển một lưu lượng lớn cho nhiều ứng dụng và nhiều người dùng.

Việc lọc gói thường không yêu cầu phải sử dụng một tường lửa độc lập bởi vì chúng thường được kèm theo trong hầu hết các bộ định tuyến có hỗ trợ TCP/IP. Dĩ nhiên, khi ta dự định sử dụng kế hoạch lọc gọi ở bộ định tuyến thì ta phải bảo đảm rằng bộ định tuyến đó là bảo mật.

Tuy nhiên, việc lọc gói không phải là một biện pháp bảo mật tốt nhất mà ta có thể sử dụng. Một trong những thiếu sót của nó là do việc lọc gói hoạt động dựa trên những địa chỉ IP chứ không dựa trên quyền đăng nhập của người dùng. Việc lọc gói chỉ cung cấp một số tính năng bảo mật đối với những hoạt động dạng "tấn công chính giữa" và không có tính năng bảo mật đối với các địa chỉ IP giả mạo. Ngoài ra, việc lọc gói còn phụ thuộc vào số cổng của gói IP và thường chỉ báo không chính xác về ứng dụng đang sử dụng, những giao thức như NFS (Network File System) lại sử dụng nhiều số cổng khác nhau gây khó khăn trong việc tạo ra những quyền bằng cách dùng phương pháp lọc tĩnh (static filtering) để điều khiển lưu lượng của chúng.

Những bộ lọc gói có thể sử dụng như một thành phần trong VPN của chúng ta do chúng có thể giới hạn lưu lượng chuyển qua một kênh để tới một mạng khác dựa trên giao thức và chiều của lưu lượng. Ví dụ: chúng ta có thể cấu hình một tường lửa dùng phương pháp lọc gói để cấm lưu lượng FTP giữa các máy tính trên mạng trong khi vẫn cho phép thông lưu lượng HTTP và SMTP giữa hai mạng.

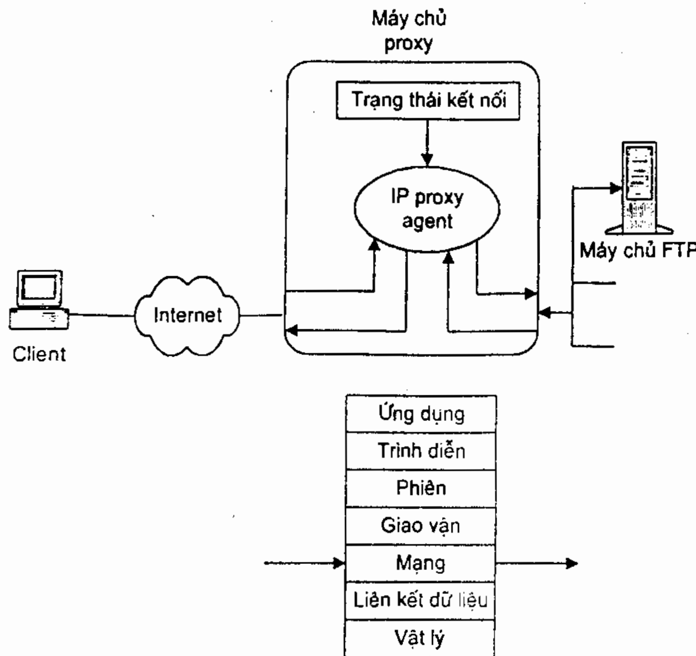
Các proxy kênh và proxy ứng dụng

Do hoạt động dựa trên thông tin địa chỉ, các bộ lọc gói được dành riêng cho một vài lớp thấp trong mô hình OSI. Hơn nữa, người ta có thể thiết ket ra những tường lửa có tính bảo mật cao hơn nếu hoạt động đồng thời trên toàn bộ các lớp trong mô hình OSI. Nguyên tắc này dẫn đến việc người ta đã tạo ra được một dạng tường lửa thứ hai là các proxy. Những tường lửa này cho phép các người dùng cùng sử dụng một proxy để liên lạc với hệ thống bảo mật, che giấu những dữ liệu có giá trị và bảo mật máy chủ khỏi tấn công của những kẻ phá hoại.

Proxy sẽ tiếp nhận một kết nối đến từ một nơi khác và nếu như kết nối này được phép, proxy sẽ tạo một kết nối thứ hai đến host đích. Trạm client sẽ cố gắng tạo kết nối sao cho đi bằng đường trực tiếp đến host này. Bởi vì các proxy có thể thực hiện trên các dạng lưu lượng và các loại gói đến từ nhiều loại ứng dụng khác nhau nên một tường lửa proxy thường được thiết kế để sử dụng những proxy agent khác, mà mỗi agent là một chương trình được viết để điều khiển một dạng chỉ

định nào đó của quá trình truyền như lưu lượng của FTP hay TCP. Chúng ta có thể muốn chuyển nhiều dạng lưu lượng thông qua proxy nên ở máy làm máy chủ proxy phải nạp và cho chạy cùng lúc nhiều proxy agent.

Các proxy kênh (circuit proxies) còn nằm ở chính các lớp TCP/IP, sử dụng kết nối IP mạng như một proxy (xem hình 10.3).



Hình 10.3: Ví dụ về một proxy kênh

So với các bộ lọc gói mà ta đã đề cập ở trước, các proxy kênh có tính bảo mật cao hơn bởi vì các máy tính bên ngoài mạng không bao giờ lấy được thông tin về các địa chỉ cũng như số cổng bên trong mạng. Một proxy kênh sẽ được cài tự động giữa bộ định tuyến mạng với Internet và proxy này sẽ đóng vai trò là đại diện cho cả mạng khi có nhu cầu liên lạc ra Internet. Các địa chỉ thật trên mạng có thể được che giấu đi bởi vì chỉ có địa chỉ của proxy là được truyền ra Internet mà thôi.

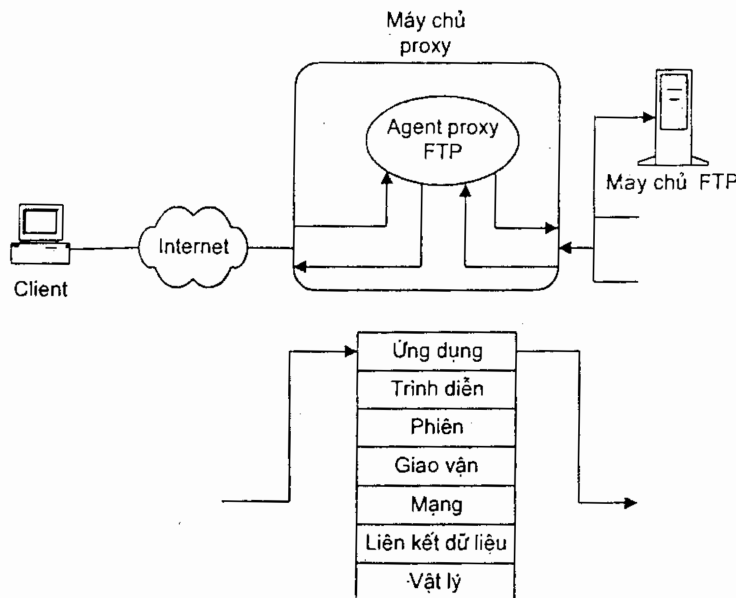
Các proxy kênh sẽ không kiểm tra dữ liệu của các ứng dụng mà việc kiểm tra này sẽ được thực hiện bởi các proxy ứng dụng (application proxy) mà ta sẽ đề cập sau. Khi một proxy kênh thực hiện một kết nối giữa một người dùng và một người dùng đích nào đó, proxy sẽ không xem xét kỹ lưu lượng qua kết nối này, điều này khiến cho proxy kênh hoạt động hiệu quả hơn so với proxy ứng dụng, nhưng cũng vì lý do đó có thể gây ra ảnh hưởng xấu đến việc bảo mật.

Nhưng ở khía cạnh khác, các proxy kênh lại chạy chậm hơn so với các bộ lọc gói bởi vì chúng phải tái tạo lại các tiêu đề IP cho mỗi gói để đảm bảo chúng đến đúng đích. Hơn nữa, các proxy kênh không có tính trong suốt đối với các

người dùng đầu cuối bởi vì chúng yêu cầu phần mềm client phải được hiệu chỉnh lại cho phù hợp.

Như chúng ta đã đề cập, các proxy ứng dụng thực hiện việc kiểm tra dữ liệu (của một ứng dụng) hiện thời trong một gói IP đang chuẩn bị được truyền đi (xem trong hình 10.4) do đó kế hoạch này ngăn cản bất cứ kẻ phá hoại nào muốn dùng các IP "giả mạo" để lấy quyền truy cập trái phép để truy cập đến mạng này. Do chức năng của một proxy ứng dụng là thuộc ở lớp ứng dụng trong mô hình OSI nên chúng còn có thể dùng cho việc xác thực cho các khoá bảo mật khác, kể cả các mật khẩu của người dùng và những yêu cầu dịch vụ.

Các tường lửa proxy thường yêu cầu phải có hai bản sao cho một agent đang dùng để chạy cho mỗi dịch vụ: một bản sao để liên lạc với các host trong mạng và bản còn lại dùng cho việc liên lạc với các host ngoài mạng. Do đó một proxy ứng dụng có thể cần hai bản sao của các HTTP, FTP, SMTP agent. Một proxy kênh hoạt động trong cơ chế tương tự, nó có thể cần một bản sao của TCP trong mạng và một bản sao dành cho ngoài mạng.



Hình 10.4: Ví dụ về một proxy ứng dụng

Do các proxy ứng dụng hoạt động như các proxy 1-1 dùng cho những ứng dụng chỉ định, chúng ta có thể cài một agent proxy cho mỗi dịch vụ IP (như HTTP, FTP, SMTP ...) mà chúng ta cần điều khiển việc truy cập đến chúng. Điều này sẽ dẫn đến hai điểm bất lợi của các proxy ứng dụng:

- Luôn tồn tại một độ trì hoãn giữa việc gia nhập của các dịch vụ IP mới trên mạng với các agent sẵn có trên mạng (tức là khi có một dịch vụ IP mới thì chúng ta phải cài thêm những agent mới cho các dịch vụ này).
- Proxy ứng dụng đòi hỏi phải xử lý nhiều trên các gói gây ra hậu quả là hiệu suất mạng sẽ bị giảm sút.

Hơn nữa, nhiều loại proxy ứng dụng yêu cầu phải hiệu chỉnh phần mềm client, mặc dù nhiều loại tường lửa sau này hoạt động mang tính trong suốt đối với các người dùng đầu cuối.

Một đặc điểm quan trọng khác của các proxy ứng dụng là dung lượng của nó dành cho các người dùng chỉ định và các trình ứng dụng. Điều này làm tăng thêm tính bảo mật đối với xác thực cho người dùng bởi vì các chứng nhận số hoặc các phương pháp bảo mật dựa trên thẻ khác có thể sử dụng cho việc chỉ định và xác thực người dùng.

SOCKS

Do các proxy hoạt động cấp độ kênh (circuit-level) có thể thực hiện tốt việc bảo mật cho nhiều mạng và do một số người dùng không muốn chịu thêm chi phí cho việc sử dụng các proxy ứng dụng có hiệu suất thấp nên người ta đã phát triển một chuẩn cho các proxy cấp kênh gọi là SOCKS. Proxy SOCKS được thiết kế chỉ để chuyển thông các lưu lượng liên quan đến SOCKS, do vậy phần mềm client cho SOCKS phải xử lý tất cả những lưu lượng vừa chuyển đến proxy để những lưu lượng này được tổ chức lại. Lưu ý: trong một proxy SOCKS thì sẽ kèm theo một proxy khác.

SOCKS được thiết kế cho những ứng dụng clien/server dựa trên nền TCP/IP, nó sử dụng một kênh dữ liệu đại diện (proxy tunnel) cho việc liên lạc giữa client và máy chủ. Trong môi trường SOCKS, một ứng dụng client sẽ đưa ra một yêu cầu đến SOCKS để liên lạc với máy chủ ứng dụng. Yêu cầu này kèm theo địa chỉ máy chủ của ứng dụng đó và phần định danh của người dùng. Sau đó SOCKS sẽ thiết lập một kênh đại diện chung đến máy chủ ứng dụng và chuyển tiếp thông tin giữa client trên với máy chủ này. Ở phiên bản 5, SOCKS có bổ sung thêm tính năng xác thực và hỗ trợ cho việc chuyển tiếp UDP. Nhìn chung, SOCKS hoạt động như một proxy cấp độ kênh nhưng có thêm một số tính năng nâng cao như tính năng kiểm tra và chỉ thị cảnh báo. Do đó, SOCKS thực hiện nhiều đặc điểm tốt hơn một tường lửa thông thường.

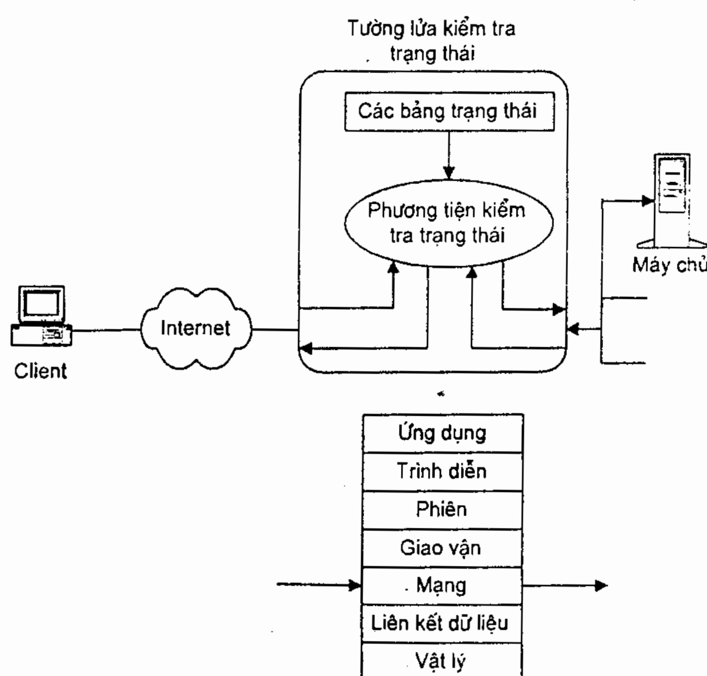
Dưới SOCKS là các trình ứng dụng client phải được mã hoá đặc biệt phục vụ cho SOCKS hay các proxy cấp ứng dụng. Một số nhà cung cấp chính về SOCKS đã cố gắng giải quyết vấn đề trên bằng cách cung cấp kèm theo một thư

viện liên kết động DLL (Dynamic Link Library) trong phần mềm client chạy trên nền Windows (lưu ý: Windows NT có hỗ trợ VPN).

Kiểm tra trạng thái

Một tường lửa lý tưởng là một tường lửa cung cấp cơ chế bảo mật tốt nhất và hiệu suất cao nhất. Người ta đã phát triển một kỹ thuật gọi là kiểm tra đa lớp trạng thái SMLI (Stateful Multi-Layer Inspection) để việc bảo mật có tính chặt chẽ hơn trong khi vẫn đảm bảo tính dễ sử dụng và chi phí thấp, vẫn đảm bảo được yêu cầu hiệu suất không bị giảm sút. SMLI là một nguyên tắc cơ sở cho những sản phẩm tường lửa thế hệ mới để chúng có thể thích ứng với nhiều loại giao thức khác nhau, với các chức năng nâng cao hơn và có nhiều đặc điểm dễ sử dụng.

SMLI cũng tương tự như một proxy ứng dụng trong trường hợp xét đến tất cả các lớp trong mô hình OSI, thay vì dùng một proxy để đọc và xử lý cho mỗi gói thông qua các logic điều khiển trên dữ liệu, SMLI sử dụng giải thuật sàng lọc lưu lượng (traffic screen algorithm) để tối ưu việc phân tích dữ liệu có thông lượng cao. Với SMLI, mỗi gói được xem xét và so sánh với những trạng thái đã biết (ví dụ như những mẫu bit) của những gói thường gặp (xem hình 10.5).



Hình 10.5: Ví dụ về một tường lửa kiểm tra trạng thái

Một trong những lợi điểm của SMLI là chỗ tường lửa sẽ đóng tất cả các cổng TCP, sau đó sẽ mở các cổng lại một cách linh động khi các kết nối có yêu cầu đến các cổng này (ví dụ như HTTP sử dụng cổng mặc định là 80). Đặc điểm này cho

phép việc quản lý các dịch vụ sử dụng đến các số cổng lớn hơn 1023 như PPTP có thể yêu cầu phải thay đổi thêm chút ít trong việc cấu hình cho các tường lửa.

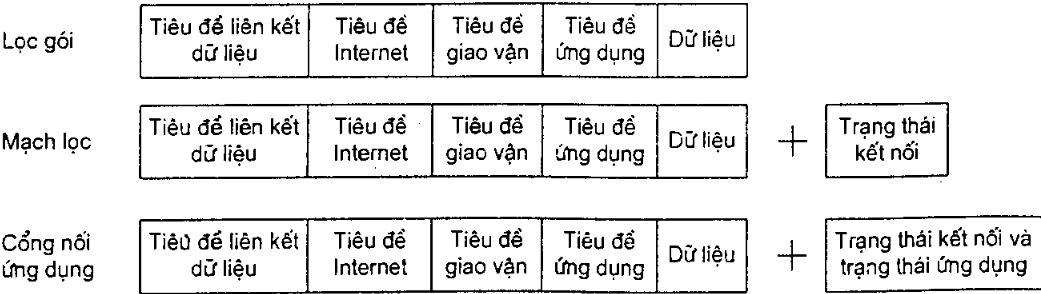
Các tường lửa kiểm tra trạng thái cũng cung cấp những đặc điểm như ngẫu nhiên hoá số tuần tự các cổng TCP và thực hiện cả việc lọc gói UDP.

Các tường lửa và số cổng

Mỗi ứng dụng TCP/IP đều được gán một số cổng riêng dùng cho việc thiết lập nên một kết nối. Đối với mô hình client/server, cả hai bên client và máy chủ đều phải có những số cổng riêng. Hầu hết toàn bộ các ứng dụng client TCP/IP đều sử dụng việc gán ngẫu nhiên số cổng lớn hơn 1023 cho việc kết thúc một kết nối. Nếu như client/server chuẩn bị liên lạc ra ngoài tường lửa thì tường lửa sẽ phải được cấu hình sao cho mở được số cổng lớn hơn 1023, hoặc client sẽ không được phép thiết lập một kết nối. Nhưng điều này sẽ gây ra những trở ngại trong việc cấu hình một số loại dịch vụ như NFS (Network File System), NIS và Netware/IP do chúng chỉ sử dụng những số cổng lớn hơn 1023. Nếu những cổng này đã trong trạng thái mở tại tường lửa để cho phép liên lạc giữa các ứng dụng client/máy chủ thì một kẻ phá hoại có thể phá vỡ được các dịch vụ còn phụ thuộc vào những số cổng lớn hơn 1023.

Các tường lửa SLMI thực sự có tính bảo mật cao, đây là nguyên nhân khiến chúng đang được sử dụng ngày càng nhiều trong những tập liên kết VPN (VPN bundles). Tuy nhiên, chúng cần phải được bổ sung với những proxy khác để hỗ trợ những tính năng quan trọng khác như xác thực (authentication).

Tổng quan về các tường lửa



Hình 10.6: Hoạt động của các proxy

Chúng ta không thể nói rằng một loại tường lửa nào đó lại hoàn toàn tốt hơn các loại khác. Đó là lý do tại sao các nhà cung cấp tường lửa ngày nay bắt đầu thực hiện những kế hoạch kết hợp: có thể minh họa như việc kết hợp giữa tường lửa SLMI với các proxy. Khi quyết định chọn loại tường lửa nào, ta phải cố gắng xác định mức độ bảo mật mà ta cần đối với lưu lượng trên mạng dựa trên những phần của gói mà một tường lửa xử lý (xem hình 10.6).

Ngoài ra, chúng ta lưu ý đến việc tường lửa của mình được tương tác với các giao thức trên mạng như thế nào (nếu có tương tác). Vấn đề này chúng ta sẽ đề cập đến chi tiết hơn ở phần kế tiếp.

Nhiều ISP khi thực hiện các dịch vụ cho VPN thì sẽ kèm theo việc quản lý cho những tường lửa như một phần trong việc thực hiện nên VPN của họ hoặc là sẽ giữ vai trò như các dịch vụ khác, sẽ cung cấp cho ta những tùy chọn (option) trong việc giám sát và quản lý các tài nguyên bên ngoài tường lửa. Nhưng nếu chúng ta đang tự chuẩn bị quản lý các tường lửa của mình thì có thể tham khảo tại các địa chỉ sau: www.cert.org, www.icsa.net.

10.1.3 Các VPN và tường lửa

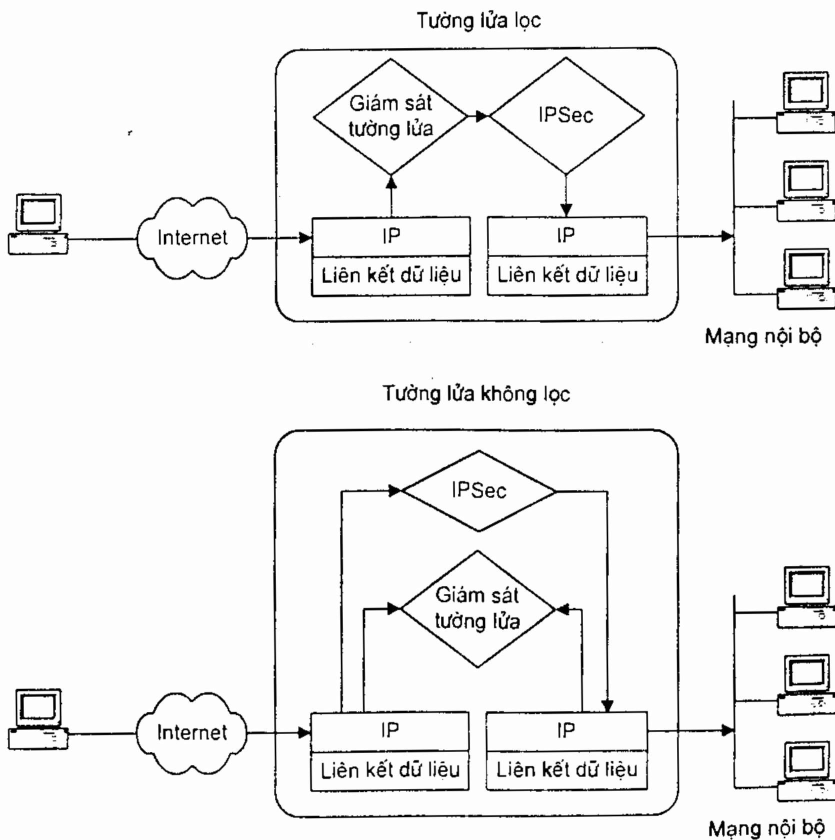
Mặc dù các tường lửa được đề cập đến như một phần trong giải pháp bảo mật cho công ty, nhưng chỉ với các tường lửa này thì không đủ xây dựng nên một VPN. Đó là vì một tường lửa không thể giám sát hay ngăn cản việc thay đổi dữ liệu có thể xảy ra khi một gói được chuyển qua Internet (tính toàn vẹn dữ liệu) và cũng không đóng vai trò là một tường lửa chung kèm theo việc mã hoá. Hơn nữa, mặc dù ta đã cài đặt việc mã hoá trên host ở tất cả các máy (minh họa như việc dùng IPSec), ta vẫn phải cần đến các tường lửa trong tổ chức mạng. Cơ chế bảo mật mạng của công ty bắt buộc phải có các tường lửa với Internet và chúng là một phần trong việc phòng thủ bên ngoài. IPSec trong mỗi máy để bàn cung cấp tính riêng tư và xác thực cho các người dùng nhưng không chắc rằng cần phải có một cơ chế bảo mật cho mạng của công ty (chẳng hạn như việc quét virus). Các tường lửa có thể bắt buộc một cơ chế giám sát phải yêu cầu những tuyến liên kết riêng giữa các mạng mặc dù các người dùng ở mỗi máy để bàn không thể hay không sử dụng một kết nối đã bị mã hoá.

Người ta thường nói đến các tường lửa như các điểm kết thúc trong một VPN logic bởi vì ta có thể quản lý toàn bộ cơ chế bảo mật của mạng thông qua duy nhất một điểm như trên. Tuy nhiên, các tường lửa là những thiết bị có tính phức tạp trong việc cài đặt và quản lý do dễ xảy ra đụng độ giữa các quyền trên mạng nếu ta không để ý trong việc thiết lập hay hiệu chỉnh trên các quyền này. Hơn nữa, việc dùng các tường lửa để thực hiện các dịch vụ bảo mật trên VPN sẽ làm tăng tính rủi ro trong trường hợp một tường lửa bị lỗi hoặc bị tổn hại do kẻ phá hoại nào đó tấn công.

Các tường lửa trong những mạng có lưu lượng cao như trong một kết nối WAN vừa phải chịu một tải nặng vừa phải xử lý lưu lượng chuyển qua chúng nên khi thêm vào chúng các chức năng như mã hoá và quản lý khoá sẽ làm cho hiệu suất của mạng giảm xuống nhiều, đặc biệt là khi có nhiều VPN đang chạy cùng lúc. Một vài tường lửa như PIX của hãng Cisco sẽ thực hiện dời việc mã hoá dữ

liệu khỏi bộ vi xử lý đến card của chúng để tăng hiệu suất cho mạng. Từ sau 1998, hãng phần mềm Checkpoint cũng đang thực hiện những biện pháp tương tự như trên, chẳng hạn công ty này đang thực hiện việc dùng một bo mạch tăng tốc Chrysalis (Chrysalic accelerator board - bo mạch này có tác dụng tăng tốc độ mã hoá) kèm với phần mềm Firewall-1 của họ. Các công ty khác cũng đang thực hiện việc gộp các phần mềm tường lửa vào trong các thiết bị phần cứng của họ, ví dụ như hãng Timestep đã cài phần mềm Firewall-1 của hãng Checkpoint vào trong hệ điều hành như một phần trong các sản phẩm cổng nối bảo mật PERMIT của họ.

Lưu lượng IPSec có thể điều khiển được bằng hai cách: hoặc là xem lưu lượng này như những gói không bị lọc, hoặc xem như những gói đã bị lọc (xem hình 10.7). Trong kế hoạch không thực hiện lọc, lưu lượng IPSec có thể được điều khiển giống như trong bộ định tuyến: dữ liệu đã được bảo mật bởi IPSec thì sẽ được truyền trực tiếp vào trong nội bộ mạng mà không xảy ra quá trình lọc hay điều khiển trên các thành phần của chúng. Còn ở phương pháp lọc, lưu lượng IPSec sẽ bị các bộ lọc của tường lửa hay các proxy xử lý trước khi chúng được phép đi vào trong mạng.



Hình 10.7: IPSec trong các tường lửa

Việc lọc lưu lượng IPSec có thể rất cần thiết nếu như cơ chế bảo mật của chúng ta chỉ cho chuyển qua một số dạng lưu lượng chính như e-mail hay FTP giữa các địa điểm trong VPN. Ngoài ra việc lọc này có thể hữu ích trong việc điều khiển lưu lượng chuyển qua các chi nhánh thương mại của công ty nếu như ta mở rộng VPN của mình đến một Extranet.

Việc bảo dưỡng những cơ chế bảo mật sao cho nhất quán thông qua những nơi khác nhau luôn luôn gặp nhiều khó khăn thách thức cho chúng ta. Việc bảo dưỡng nhất quán cho những tường lửa tại mọi nơi là điều thật sự quan trọng bởi vì các tường lửa này điều khiển việc truy cập đến nhiều nơi và từ nhiều vị trí. Việc cấu hình và truy cập đến các quyền phải giống nhau ở các tường lửa trong công ty. Nhưng có nhiều tường lửa yêu cầu phải được cấu hình cẩn thận bằng phương pháp thủ công bởi những người quản trị tại mỗi địa điểm này khi cập nhật những bản sao cho toàn bộ các quyền. May mắn là một số tường lửa có thể thực hiện việc bảo dưỡng những quyền bảo mật của chúng và các tệp cho việc cấu hình có thể được sao chép từ một tường lửa này đến những tường lửa khác khiến cho công việc quản lý của ta trở nên dễ dàng hơn. Tuy vậy, ta nên lưu ý rằng nếu các tệp dùng cho việc định cấu hình của tường lửa có thể được chuyển đi và cài đặt tại các tường lửa khác thì ta sẽ gặp một vấn đề cần quan tâm là phải bảo đảm tính bảo mật cho các tệp này.

Điều này có thể thực hiện bằng cách chuyển trực diện thông qua một giao ước trước hay bằng cách gửi e-mail bảo mật, nhưng ta phải đảm bảo tính bảo mật trong việc chuyển giao và điều khiển các tệp trên.

Các tường lửa và việc truy cập từ xa

Do các tường lửa có sẵn những cơ chế xác thực người dùng mạnh nên chúng có thể thực hiện thêm được những tính năng khác bằng cách phục vụ như một tiêu điểm cho các người dùng vào mạng bằng cách quay số. Hầu hết các tường lửa đều có thể kiểm tra định danh của người dùng và thiết lập một phiên làm việc được mã hoá giữa tường lửa và máy tính của những người dùng quay số trên để bảo mật tính tin cậy cho dạng thức truy cập kiểu quay số trong VPN.

Để thực hiện việc làm trên, các người dùng đầu xa (người dùng từ xa) phải cài một phần mềm thích hợp trên các máy tính của họ. Nếu chúng ta đang định kế hoạch một tường lửa dùng cho các đầu cuối sử dụng PPTP hoặc L2TP, tất cả những người dùng của ta phải cần một phần mềm client sử dụng giao thức PPP để họ có thể quay số đến các ISP của họ. Dù rằng client PPTP trên không cung cấp mức độ bảo mật tin cậy nhất cho những dữ liệu nào được truyền tải giữa client và máy chủ của công ty mình, nếu ta muốn có mã hoá tốt hơn, ta phải cần cài client PPTP hay L2TP trong những máy tính của những người dùng đầu xa này.

Như chúng ta đã đề cập đến trong phần trước, thị trường hiện tại có xu hướng dùng PPTP và L2TP cho những VPN quay số (dial-in VPN) và dùng IPSec cho những VPN kết nối LAN-WAN (LAN-to-WAN VPN). Tuy nhiên IPSec cũng thật sự thích hợp cho các VPN quay số. Một số nhà cung cấp tường lửa đã viết những phần mềm client đầu xa sử dụng IPSec. Do IPSec không phải là cách chuẩn cho việc xác thực người dùng, các client đầu xa dùng IPSec thường dành riêng cho những nhà cung cấp. Điều này có nghĩa là chúng ta phải có phần mềm client đầu xa tương thích với tường lửa của nhà cung cấp và vì vậy tối thiểu trong thời gian gần nhất, ta sẽ bị lệ thuộc vào một nhà cung cấp để tránh những rắc rối trong vận hành. Điều này trở nên thật sự quan trọng nếu mạng di động của ta thường xuyên truy cập đến nhiều vị trí trong VPN. Tương tự, mỗi vị trí trong mạng (VPN site) phải cài đặt một tường lửa giống nhau với cùng những tùy chọn cho VPN. Dĩ nhiên, việc sử dụng những tường lửa giống nhau tại mỗi vị trí làm cho việc quản trị cho cơ chế bảo mật hoạt động tốt hơn.

10.1.4 Những yêu cầu đối với tường lửa

Nếu chúng ta dự định dùng một tường lửa như một cổng nối cho mạng VPN của mình, thì ta cần phải xem xét những vấn đề chính cần thiết. Trước tiên, chúng ta sẽ nhìn lại một số yêu cầu chung, sau đó sẽ thảo luận đến những yêu cầu liên quan đến IPSec, cuối cùng sẽ tìm hiểu các vấn đề xung quanh PPTP và L2TP.

Những yêu cầu chung

Bất kể việc VPN của chúng ta sử dụng giao thức nào thì ta cũng phải cần phải xem xét việc tường lửa tích hợp với các phần còn lại trong cơ chế bảo mật và việc quản trị mạng của ta ra sao. Ví dụ như, nhiều hệ thống dùng PPTP và L2TP còn tùy thuộc vào RADIUS hay các hệ thống dựa trên thẻ trong việc xác thực người dùng. Nếu ta đã sẵn sàng sử dụng một hệ thống riêng để xác thực cho các người dùng đầu xa thì ta có thể đơn giản việc truyền bằng cách sử dụng một tường lửa tương thích với hệ thống hiện tại của mình. Ngoài ra, nếu ta cảm thấy cần thiết phải tăng độ bảo mật cho hệ thống xác thực, thì có thể cài thêm một hệ thống hai nhân tố (two factor system) như SecurID. Phương pháp xác thực của một tường lửa có thể trở nên kém hơn một nhân tố riêng khác như nhiều nhà cung cấp tường lửa đã từng gộp những hệ thống xác thực mạnh trong các sản phẩm của họ. Nhưng dù gì chăng nữa, tính tương thích của hệ thống vẫn có vai trò quan trọng. Việc thực hiện các IPSec vẫn xảy ra tình huống tương tự như vậy, mặc dù IPSec không được chuẩn hoá trong một phương pháp xác thực riêng biệt và đa số những giải pháp này là được dành riêng cho những nhà cung cấp.

Nếu chúng ta đang định kế hoạch dùng một hệ thống xác thực dựa trên những chứng nhận số (digital ceritificates) thì ta phải biết các chứng nhận này sẽ

được phân phối và xác thực như thế nào? Chúng ta sẽ có dịp đề cập đến vấn đề này một cách chi tiết hơn trong phần "Quản lý bảo mật".

Trong tương lai, cần thiết phải thống nhất trong việc quản lý đối với băng thông, chất lượng dịch vụ QoS, truy cập từ xa, truy cập đến các máy chủ và các tài nguyên khác trên mạng khi số lượng quyền của người dùng tăng lên sẽ sử dụng việc quản lý trên cơ sở chính sách (policy-based management). Việc quản lý trên cơ sở chính sách tùy thuộc vào những hệ thống phân tán trong việc định danh và việc xác thực người dùng để việc quản lý được dễ dàng hơn.

Điểm cuối cùng, nhưng không kém phần quan trọng, ta nên nhớ rằng nếu muốn cài đặt nhiều tường lửa tại nhiều vị trí, ta có thể phải bảo dưỡng một chính sách bảo mật chặt chẽ hơn nếu như tường lửa ta chọn hỗ trợ việc quản trị đồng bộ cho nhiều vị trí. Người quản trị tại những nơi này có thể cần trao đổi các tệp như chúng ta đã đề cập ở phần trước hay thông qua những dạng quản lý từ xa khác. Nếu một sản phẩm có kèm theo khả năng quản lý từ xa, ta phải đảm bảo tính bảo mật trong việc truy cập từ xa đến tường lửa.

IPSec

Vì phần lớn mục đích của IPSec đều xoay quanh việc sử dụng các chức năng mật mã hoặc cho việc mã hoá hoặc cho xác thực gói, điều này thật sự quan trọng để đảm bảo rằng một tường lửa không chỉ hỗ trợ những giải thuật chính xác mà còn hỗ trợ những tiến trình lệ thuộc như việc tái định khoá và những tiến trình kết hợp bảo mật. Ngoài ra, do các chuẩn cho IPSec hiện đang nâng lên phiên bản 2, ta phải thận trọng điều tra tính tương thích của mỗi sản phẩm đối với những đặc điểm của phiên bản 2 này, phiên bản này cung cấp tính bảo mật và độ linh động cao hơn.

Phần lớn các thiết bị bảo mật đều hỗ trợ các kết nối mạng khác nhau đối với các lưu lượng chưa bị mã hoá và lưu lượng đã bị mã hoá, điều này cho phép ta cung cấp những kết nối cho cả hai loại lưu lượng và bảo dưỡng chia cắt vật lý giữa những mạng đã được mã hoá với nhiều mạng mở khác. Những thiết bị bảo mật sẽ từ chối tất cả những gói không có phần tiêu đề chính xác (ví dụ như tiêu đề IPSec), những gói này sẽ được gửi đến một mặt phẳng đã mã hoá và có thể được chấp nhận nếu chúng thuộc những giao thức chuyển giao khoá.

Bây giờ chúng ta thử kiểm tra lại những giải thuật mã hoá nào mà một tường lửa trong VPN có thể hỗ trợ. Khi chấp nhận rủi ro ở mức trung bình, ta chỉ cần sử dụng giải thuật DES CBC mặc định (dùng cho việc mã hoá) và những giải thuật chia nhỏ HMAC-MD5 hoặc HMDA-SHA-1 (dùng cho việc xác thực) là đủ.

Mặc dù IPSec yêu cầu tối thiểu phải sử dụng việc định khoá bằng nhân công, ta cũng nên xem xét những sản phẩm cho phép việc thay đổi các khoá mã một cách tự động và theo chu kỳ hoặc khi có một kết nối mới được thiết lập. Nếu như điều

khiển liên kết trở thành mối lo ngại, ta không nên kết thúc đối với một hệ thống chuyển giao khoá độc quyền, nhưng nhất định phải kết thúc trong những hệ thống đã nêu trong IKE (xem thêm trong phần "Sử dụng IPSec để xây dựng một VPN"). Việc tái định khoá tự động trong tương lai sẽ củng cố thêm cho việc bảo mật lưu lượng của ta bằng cách tạo ra thêm những khó khăn cho những tay bẻ khoá (hacker) khi khoá bị chặn (ví dụ như khi một kẻ tấn công phải dành ra một khoảng thời gian để bẻ khoá, sau khi lấy được một khoá thì lúc này khoá đã hết hạn sử dụng. Do đó kẻ tấn công có lấy được khoá vẫn không sử dụng khoá này được do nó đã hết hiệu lực). Ngoài ra, hãy tin chắc rằng một tiêu đề IPSec sẽ được tường lửa sử dụng đến. Mặc dù các chuẩn IPSec nguyên bản không yêu cầu hỗ trợ cả hai tiêu đề AH và ESP, nhưng chúng thích hợp cho việc áp dụng cho cả hai loại tiêu đề trên cho mỗi gói. Một vài thiết bị phục vụ IPSec chỉ hỗ trợ tiêu đề xác thực AH.

Bởi vì các liên kết bảo mật có tính quyết định đối với hoạt động của IPSec ta có thể tự nhập vào các liên kết bảo mật này, thường từ một tệp tương tự như S/WAN đã khuyến nghị.

Tường lửa thường được xem như một thiết bị bảo mật có kèm theo việc bảo mật các khoá mã và các khoá dùng riêng (private keys) sử dụng bởi một thiết bị. Khi một người vô tình truy cập được vào tường lửa vẫn không thể lấy được các khoá này.

Đối với các đặc điểm nguyên gốc của IPSec, thì không có một hệ thống nào có thể thực hiện việc chống cự lại trong trường hợp bị một kẻ phá hoại tấn công chặn đứng một loạt các gói và các gói này sẽ phải được truyền lại sau đó. Tuy nhiên, các chuẩn tái bản của IPSec mà đã được IETF phê duyệt sau năm 1998 có kèm theo việc một dịch vụ khử việc phát lại, đầu thu có thể được yêu cầu dịch vụ này để tăng thêm sức phản công đối với các hành động tấn công vào những dịch vụ bị từ chối hoạt động dựa trên việc truyền lại. Để cung cấp thêm tính bảo mật cho VPN của mình, chúng ta nên xem qua các sản phẩm nào của nhà cung cấp có hỗ trợ hệ thống antireplay mới này hay không, thay vì ta cứ phải dùng những biến thể không thuộc chuẩn.

Như chúng ta đã từng đề cập, mọi thiết bị bảo mật sẽ có phương pháp riêng trong việc ghi nhận các biến cố bảo mật và tường thuật lại các biến cố này. Nếu có thể, ta hãy kiểm tra xem hệ thống có thể khởi tạo một vài dạng cảnh báo khi có một vài hoạt động liên tiếp luôn chiếm chỗ như việc chỉ ra lỗ hổng trong cơ chế bảo mật chẳng hạn.

Mặc dù có thể ta cảm thấy chế độ giao vận (transport mode) dùng cơ chế bảo mật IPSec là đủ bảo mật cho dữ liệu của mình, nhưng để chắc hơn, ta có thể cần một cơ chế bảo mật bảo mật hơn bằng cách dùng chế độ đường hầm (tunnel

mode). Cần biết thêm là một tường lửa có thể hỗ trợ cả hai chế độ trên.

PPTP và L2TP

Do PPTP và L2TP quan niệm rằng các đường hầm kết cuối tại một máy chủ mạng, các tường lửa thường không được sử dụng như một điểm kết thúc cho các đường hầm trên. Thay vào đó, bất kỳ một tường lửa nào cài trên mạng sẽ được cấu hình để chuyển lưu lượng từ PPTP hoặc L2TP bằng cách sử dụng số cổng chính xác cho nó. Lưu lượng PPTP sử dụng cổng TCP là 1723 và số này không được thay đổi và L2TP sử dụng cổng mặc định là 1701. Đối với L2TP thì không đòi hỏi cần phải gán một cổng cố định cho nó trong việc chuyển các lưu lượng L2TP. Những nhà quản trị mạng sẽ có tùy chọn trong việc chọn những số cổng khác nhau để chuyển lưu lượng L2TP, điều này có thể làm cho những kẻ phá hoại gặp nhiều khó khăn hơn trong việc đột nhập vào mạng thông qua những cổng thông thường đã biết.

Hãng Microsoft đã thực hiện chính máy chủ PPTP trên hệ điều hành mạng Windows NT server của họ, trong cấu hình của máy chủ PPTP này chúng ta có thể cho phép hoặc không cho phép thực hiện việc lọc gói. Nếu việc lọc gói được cho phép trong một máy chủ đang chạy RRAS, thì sẽ chỉ có những gói PPTP mới được phép chuyển qua mà thôi.

10.1.5 Tổng quan về các sản phẩm

Do các tường lửa thường được xem như một vị trí logic để kết thúc những đường hầm VPN và là một yếu tố bắt buộc trong cơ chế bảo mật, do đó hiện nay các tường lửa có tính tương thích hơn với VPN nếu so với các thiết bị khác lớp trong VPN. Như ta có thể thấy trong bảng 10.1, một số tường lửa thực ra là những phần mềm được thiết kế để chạy trên các hệ điều hành khác nhau chẳng hạn như Unix và Windows NT và một vài tường lửa là những thiết bị phần cứng có thể được cấu hình thông qua hầu hết các máy trạm.

Bảng 10.1: Các sản phẩm tường lửa dành cho VPN

	1	2	3	4	5	6
Sản phẩm (Công ty)	Aix (IBM)	Eagles (Raptor)	Permit 2505 (Timestep)	Pix (Cisco)	Proxy (Microsoft)	Efs (Sun)
Giá	$4945-$16495	$65004	$4995-$10995	$9000 (64 kết nối) $15000 (256 kết nối)	$995	$4995
Giao thức đường hầm	IPSec, L2PT	IPSec, swIPc	PPTP, L2TP, L2F	IPSec (ESP)	PPTP	SKIP

	1	2	3	4	5	6
Phần mềm máy chủ	AIX, OS/2, Win NT	Win NT 4.0, Solaris, Unix	Không	Không	Win NT	Solaris, Win95
Phần mềm truy cập từ xa	Win95, NT,OS/2 Warp	Win3.11, Win95, NT	Win95	[illegible]	Win95,NT	Solaris, Win95, NT
Giao thức được hỗ trợ	IP, IPX	TCP, UDP, ICMP	TCP, UDP	TCP, UDP	TCP, UDP	TCP, UDP
Kiểu mã hoá	IPSec, DES, CDMF	DES, Triple, DES, RC2, IPSecAH	DES, Triple, DES, IPSec, FWZ-1	DES	MPPE, PPP	RC2, RC4, DES, Triple DES, 128bit SAFER OBO
Xác thực người dùng		S/Key, NT Domain, RADIUS, TACACS+ Crypocard, SecurID	S/Key, SecurID, Axent	RADIUS, TACACS+	RADIUS	SKIP, Password SecurID
Điều khiển truy cập	Nguồn, đích, giao thức, địa chỉ IP, cổng, người dùng, thời gian	Nguồn, đích, địa chỉ IP, dịch vụ	Nguồn, đích, dịch vụ, người dùng, thời gian	RADIUS, TACACS+	Địa chỉ IP, nguồn, đích	Nguồn, đích, địa chỉ IP, ứng dụng
Tổ hợp quản trị người dùng		Tường lửa người dùng, miền người dùng NT	RADIUS	Miền người dùng NT, LDAP, RADIUS	Miền người dùng NT	Mật khẩu Unix, SecurID
Quản lý khoá	Nhân công, độc quyền	Độc quyền	IKE, SKIP, FWZ, nhân công, IPSec	Nhân công	N/A	SKIP
Các nút được hỗ trợ		Không giới hạn				

	1	2	3	4	5	6
Các đường hầm được hỗ trợ		Không giới hạn		256		
Quản trị từ xa	Có		Có	Có	Có	Có
Chứng nhận					Không	Không
Client truy cập từ xa	Có	Có	Có	Không	Có	Có
Dịch địa chỉ mạng (NAT)	Có			Có		Có
Loại sản phẩm	Phần mềm	Phần mềm	Thiết bị tường lửa	Phần cứng	Phần mềm	Phần mềm

Bây giờ chúng ta sẽ xem xét các hệ điều hành cho tường lửa thì khác nhau như thế nào? Một khi nói đến vấn đề bảo mật, thì có nhiều điều để bàn đến. Theo cách truyền thống, hầu hết các tường lửa sẽ được thảo chương (ta nói đến các tường lửa dạng phần mềm) để phục vụ riêng cho các hệ điều hành và những lỗ hổng trong cơ chế bảo mật đã được tìm thấy chung trong nhiều máy trạm và máy chủ của hệ điều hành đó, chẳng hạn như Windows NT và Unix - tức là người ta đưa ra những biện pháp khắc phục những thiếu sót, yếu điểm trong bảo mật của hệ điều hành mà trong quá trình sử dụng họ phát hiện ra hay người dùng phản ảnh về cho nhà sản xuất. Tuy nhiên, các nhà cung cấp đang thực hiện những phần mềm tường lửa có thể chạy cùng trên nhiều hệ điều hành phổ biến kèm theo những đoạn mã để giải quyết những lỗ hổng trong việc bảo mật đã biết. Nếu bàn đến vấn đề hiệu năng thì Unix có thể mạnh hơn Windows NT (Unix chạy nhanh và có độ ổn định, độ bảo mật cao hơn Windows NT), nhưng chúng ta không đề cập chi tiết hơn trong những chỉ tiêu chuẩn, bởi vì các điểm chuẩn đang thay đổi từng ngày (ví dụ tuy một số khách hàng thích tính ổn định của Unix nhưng lại không thích giao tiếp với những dòng lệnh và những tham số lệnh rắc rối của chúng, do đó họ chọn Windows thay cho Unix vì Windows có giao diện người dùng sử dụng kỹ thuật đồ họa - GUI (Graphic User Interface) - nên Windows có tính gần gũi, dễ sử dụng hơn Unix).

Khi chúng ta nhận được một danh sách các sản phẩm ứng cử cho VPN của mình, nên nhớ rằng thị trường sản phẩm này không đứng yên mà luôn thay đổi từng ngày (cũng như thị trường máy tính hiện nay vậy: càng ngày càng có nhiều máy tính mạnh hơn, giá cả lại rẻ hơn!) và những sản phẩm có phiên bản mới hơn sẽ kèm theo những tính năng sửa đổi hay các tính năng mới. Nói cách khác, ta có thể sử dụng bảng 10.1 như một gợi ý, nhưng nó chỉ có giá trị của năm 1998.

Lưu ý rằng có nhiều nhà cung cấp bộ định tuyến và các thiết bị phần cứng khác dùng cho VPN đã bắt đầu tích hợp các tường lửa vào những sản phẩm của họ, hai tường lửa tích hợp nổi tiếng là Firewall-1 của hãng phần mềm Checkpoint và Gauntlet của hãng Associates.

Việc sử dụng các tường lửa để tạo ra các VPN là một giải pháp có tính khả thi đối với một số mạng, những VPN dựa trên tường lửa là giải pháp thích hợp nhất cho các mạng nhỏ, lưu lượng truyền dữ liệu nhỏ (khoảng 1-2Mbit/s khi ra một liên kết WAN) và ít biến động (ví dụ như không cần phải cấu hình thường xuyên). Nếu ta muốn đạt hiệu suất cao hơn, thì phải dùng đến những giải pháp khác.

Một vài công ty khác như Checkpoint hiện nay đang xúc tiến ý tưởng điều khiển lưu lượng, bao gồm các công việc như quản lý băng thông và chất lượng dịch vụ (QoS). Việc tích hợp điều khiển lưu lượng với xác thực và điều khiển truy cập còn có ý nghĩa lâu dài, cũng như việc quản trị mạng dựa trên chính sách đang trở nên phổ biến hơn (và hữu ích nữa). Chúng ta chỉ mới bắt đầu xem xét những bước đầu tiên trong việc tích hợp các chức năng của quản lý mạng và thực hiện việc quản lý dựa trên chính sách đối với những mạng của công ty và chúng chắc chắn sẽ được triển khai rộng rãi trong vài năm tới.

10.2 Bộ định tuyến

Nếu như các tường lửa giống như một vị trí logic đối với việc cài đặt những chức năng cho VPN thì bộ định tuyến có nhiều vai trò hơn. Các bộ định tuyến phải kiểm tra và xử lý mỗi gói khi chúng vào/ra khỏi LAN.

Chúng ta đang bàn về một phương pháp để cho các bộ định tuyến có thể được sử dụng để bảo mật mạng LAN khỏi tầm tấn công của những kẻ phá hoại, cách đó là dùng bộ định tuyến kèm với việc lọc gói (nên lưu ý rằng chuyển tiếp trong lọc gói của một bộ định tuyến đối với một phần hay toàn bộ trong việc bảo mật tường lửa có nghĩa là bản thân bộ định tuyến phải có tính bảo mật). Tuy nhiên, lọc gói không đủ để bảo mật đối với nhiều dạng tấn công có thể xảy ra trên mạng, đây là một trong những lý do tại sao người ta đã phát triển lên nhiều dạng tường lửa khác. Trong phạm vi của VPN, loại bộ định tuyến hiện đang được ưa chuộng nhất là các bộ định tuyến mã hoá (encrypting router).

10.2.1 Những yêu cầu đối với bộ định tuyến

Một bộ định tuyến mã hoá phải cần thỏa mãn một số yêu cầu cũng như ta đã từng đề cập trong trường hợp tường lửa. Nhìn chung, chúng thực hiện những chức năng tương tự nhau và chỉ là những chức năng phụ trợ trong mạng. Do những yêu cầu này tương tự nhau, ở đây chúng ta chỉ thực hiện việc liệt kê lại chúng một cách ngắn gọn mà thôi.

Các bộ định tuyến mã hoá được dành riêng cho các VPN nếu như chúng thực hiện những công việc sau:

- Bao gồm cả việc mã hoá và giải mã lưu lượng đối với những kết nối mạng riêng biệt.
- Ít nhất phải hỗ trợ được những giải thuật mã hoá IPSec mặc định (DES CBC, HMAC-MD5 và HMAC-SHA-1).
- Hỗ trợ chiều dài khoá mã tối ưu nhất đối với yêu cầu bảo mật của chúng ta.
- Cho phép cấu hình kết hợp bảo mật bằng nhân công.
- Hạn chế việc truy cập đến các khoá.
- Hỗ trợ việc tái định khoá một cách tự động theo chu kỳ hoặc mỗi khi có một kết nối mới.
- Hỗ trợ cơ chế khử phát lại (antireplay) của IPSec phiên bản 2.
- Thực hiện việc ghi nhận lại các lỗi khi xử lý các tiêu đề và báo động đối với việc lặp đi lặp lại những hoạt động không cho phép.
- Hỗ trợ cả hai chế độ giao vận và chế độ kênh của IPSec.

Chúng ta nên lưu ý rằng có nhiều quan điểm khác nhau về IPSec đối với những điểm mà ta đã liệt kê ở trên, nhưng IPSec có khả năng thực hiện được hầu hết các chức năng bảo mật cho các hệ thống VPN. Một vài bộ định tuyến hỗ trợ một trong hai giao thức PPTP và L2TP đối với việc định đường hầm, trong mỗi trường hợp các yêu cầu đối với việc liên điều khiển có thể ít hơn những gì được liệt kê như trong bảng 10.2. Bởi vì L2TP có thể dùng kèm với IPSec để thực hiện mã hoá - như ta đã đề cập trong phần giới thiệu tổng quan: các giao thức chính để xây dựng nên VPN, các bộ định tuyến có khả năng L2TP sẽ được xem xét như những bộ định tuyến có khả năng IPSec.

Do các bộ định tuyến được thiết kế một cách tổng quát để kiểm tra các gói tại lớp mạng - lớp thứ 3 - trong mô hình OSI (bộ định tuyến hoạt động tại lớp mạng) và không dùng để xác thực người dùng, chúng ta cần phải có thêm một máy chủ xác thực cho bộ định tuyến mã hoá của mình trong việc tạo ra một VPN có tính bảo mật. Nếu ta chưa sẵn sàng trong việc sử dụng một hệ thống xác thực dành cho việc truy cập từ xa, hãy tham khảo đến PAP hoặc CHAP hay có thể dùng ExpressRouter của hãng Intel. Tuy nhiên chúng có tính xác thực kém hơn so với một hệ thống xác thực chuyên dụng như trên. Tốt nhất, ta nên dùng một hệ thống hai nhân tố như SecurID hoặc CryptoCard đã từng cung cấp. Có nhiều hệ thống được thiết kế để hoạt động với các bộ định tuyến mã hoá, nhưng ta phải kiểm tra tính tương thích của chúng đối với bộ định tuyến của mình.

Bảng 10.2: Các bộ định tuyến có khả năng dùng được cho VPN

Sản phẩm (Công ty)	Intel Express router VPN (Intel)	IOS 11.3 (CISCO)	MicroRouter series, RISC, Router 3500, 3800 (hệ thống tương thích)	2210 Nways Multi-protocol router (IBM)	NetBuilder II routers (3COM)	VPN500 series (Bay Network)
Giá	$1299-$5999	$500-$7000	Microrouter $1895-$2695 RISC router $3995-$4495	$2800-$3800	$10004	500n: $3995 550n: $4995
Giao thức đường hầm	Độc quyền	L2F	IPSec, GRE	L2TP, IPSec	PPTP, L2TP	IPSec
Giao thức	TCP, UDP, IPX	TCP, UDP, IPX	TCP, UDP, IPX	TCP, UDP, IPX	TCP, UDP, IPX	TCP, UDP
Mã hoá	144 bit - Blowfish	DES	RSA, DES	IPSec	IPSec, MPPE	DES, Triple DES
Xác thực	PAP, CHAP	RADIUS, TACACS +	CHAP, PAP, RADIUS		PAP, CHAP, RADIUS, ACE, miền NT	ACE, RADIUS, CHAP
	Có	Có	Có		Có	Không
Nén	Có	Có	Có		Có	Có
	Có			Có	Có	Có

10.2.2 Tổng quan về các sản phẩm

Nếu như chúng ta so sánh giữa bảng liệt kê sản phẩm 10.1 và 10.2, chúng ta sẽ thấy số lượng sản phẩm bộ định tuyến mã hoá ít hơn nhiều so với số lượng tường lửa. Một lý do của sự chênh lệch này là do có nhiều thiết bị phần cứng tích hợp sẵn cho VPN.

Mặc dù phần lớn các sản phẩm được liệt kê trong bảng 10.2 hỗ trợ một hay nhiều các chuẩn mà ta đã giới thiệu như PPTP, L2TP, L2F, IPSec. Lưu ý rằng bộ định tuyến của hãng Intel sử dụng một thiết kế độc quyền cho định đường hầm. Ngoài ra nó còn sử dụng giải thuật Blowfish cho việc mã hoá, tuy giải thuật này tốt nhưng nó không có trong những chuẩn khác. Do bộ định tuyến của hãng Intel là sản phẩm mang tính độc quyền, nên nó không thể sử dụng chung với các bộ định tuyến khác để tạo nên một VPN, thay vào đó, mọi vị trí trong VPN của chúng ta phải cùng cài đặt bộ định tuyến nhanh của hãng Intel.

Như chúng ta đã nói trước đây, ta không thể đề cập hết những đặc điểm của sản phẩm do càng ngày các công ty càng thêm những đặc điểm mới cho sản phẩm của họ cũng như thực hiện sửa đổi trên những đặc điểm đã có. Ví dụ, mặc dù hiện nay bộ định tuyến của IBM hỗ trợ L2TP như một giao thức định đường hầm, nhưng công ty IBM đang thông tin rộng rãi rằng những bộ định tuyến này sẽ hỗ trợ thêm giao thức IPSec trong thời gian ngắn sắp tới.

Cũng như các tường lửa, các bộ định tuyến có thể gây ảnh hưởng đối với hiệu suất mạng trong lúc phải thực hiện những chức năng bổ sung của VPN, đơn cử như việc mã hoá các gói. Bộ điều hợp dịch vụ mã hoá ESA (Encryption Service Adapter) của hãng Cisco là một cách giải quyết cho vấn đề hiệu suất trên. ESA là một phương tiện mã hoá dựa trên một chip đồng xử lý để làm giảm bớt việc xử lý của bộ định tuyến.

Ngày nay, bộ định tuyến đang được thực hiện để làm nhiều công việc trên mạng, không những chúng được sử dụng để điều khiển các kênh VPN mà còn dùng để điều khiển việc cung cấp chất lượng dịch vụ (QoS) trên mạng. Ngoài ra, một chức năng mới của bộ định tuyến là định tuyến dựa trên chỉ số QoS và các VPN, có thể làm giảm đi thay vì nâng cao hiệu suất mạng. Bộ định tuyến vẫn được xem như các thiết bị logic để điều khiển nhiều chức năng khác nhau, do đó ta cần phải cân bằng công suất tính toán của bộ định tuyến. Và nói thêm về bộ ESA của hãng Cisco, có thể đáp ứng với những công việc mới mà ta muốn bộ định tuyến thực hiện.

Bởi vì các bộ định tuyến không thể thực hiện được toàn bộ các chức năng của một VPN như việc xác thực người dùng, nên nhiều nhà cung cấp bộ định tuyến đã tích hợp vào bộ định tuyến những phần mềm tường lửa. Ví dụ, hãng Bay Networks đã tích hợp phương tiện INSPECT (lấy từ tường lửa của hãng phần mềm Check Point) vào phiên bản 11.02 của Bay Router Services OS.

TỔNG KẾT

Tường lửa có ba loại chính: các bộ lọc gói, proxy và các hệ thống kiểm tra trạng thái. Mỗi loại khác nhau về mức bảo mật mà chúng cung cấp, cũng như về vấn đề hiệu suất và mức độ phức tạp trong việc cấu hình. Nhìn chung, nếu một tường lửa càng có tính bảo mật cao thì nó sẽ càng chạy chậm và chúng ta muốn loại tường lửa nào thực hiện đủ các yêu cầu về bảo mật cho mạng LAN của mình, do đó ta nên thường xuyên tìm những nhà cung cấp tường lửa đang tích hợp nhiều phương pháp khác nhau vào một sản phẩm duy nhất của họ để ta có được một cơ chế bảo mật tốt nhất dành cho mạng của mình.

Cả tường lửa và bộ định tuyến đều có thể sử dụng như những phần tử khoá trong việc tạo ra một bức tường lửa ngăn cản những xâm nhập bất hợp pháp. Hiện nay các tường lửa tương thích VPN có tính đa dạng hơn so với các bộ định tuyến và trong tương lai cũng sẽ như vậy, bởi vì ý định thêm vào một chức năng bảo mật (ví dụ như trong việc mã hoá và định đường hầm cho VPN) cho một cơ chế bảo mật khác (ví dụ như cơ chế bảo mật vòng ngoài) có ý nghĩa đối với nhiều khách hàng. Tuy nhiên, phải chú ý đến những vấn đề cản trở đến việc đạt hiệu suất cao đối với việc kết hợp những chức năng của tường lửa và bộ định tuyến và thông lượng hữu dụng có thể không đủ cho các liên kết tốc độ cao của mình. Việc thêm vào các card đồng xử lý trong việc mã hoá cho các tường lửa trong VPN có thể giải quyết được vấn đề hiệu suất trong VPN.

Một số ít các bộ định tuyến hoạt động độc lập - tức không tích hợp tính năng tường lửa trong nó - có thể sử dụng để tạo ra những VPN. Chúng thường phải được hỗ trợ với các sản phẩm khác, như các máy chủ xác thực để có thể tạo ra một VPN hoàn chỉnh. Hơn nữa, chúng ta sẽ thấy trong phần kế, có nhiều thiết bị phần cứng tích hợp kèm theo tính năng định tuyến, đang được sử dụng cho các VPN.

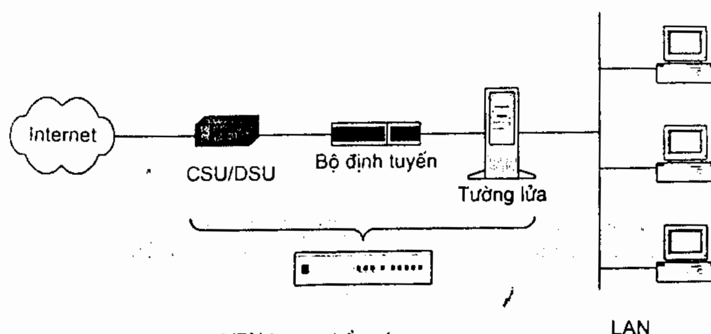
CHƯƠNG 11

PHẦN CỨNG CỦA VPN

Trong chương 9, 10 đã đề cập đến một số sản phẩm đang được sử dụng phổ biến, tường lửa hoặc bộ định tuyến là những khối chính xây dựng nên một VPN. Và như chúng ta đã thảo luận, mỗi lớp sản phẩm đều có một vài thiếu sót nào đó. Mặc dù nhiều sản phẩm tương thích với những mạng nhỏ, với các nhu cầu về băng thông ở từ mức thấp đến mức trung bình, thì vẫn có rất ít sản phẩm có thể điều khiển các liên kết WAN ở tốc độ Ethernet (10 Mbit/s hay 100 Mbit/s - đối với Fast Ethernet) hay tốc độ T3 (44.736 Mbit/s). Hơn nữa, nhiều sản phẩm cần phải dùng kết hợp với các sản phẩm của những công ty khác để có thể cung cấp được toàn bộ các tính năng cho VPN, từ việc xác thực đặc biệt cũng như việc mã hoá và định đường hầm.

Nhắc lại rằng một số vị trí trong mạng thích hợp đối với việc thực hiện những chức năng cơ bản của một VPN, đặc biệt khi ta phải sử dụng các sản phẩm khác nhau cho các chức năng khác nhau. Một số đoạn thị trường phát triển nhanh nhất đang tìm kiếm việc cung cấp giải pháp cho VPN bao gồm những nhà cung cấp đang thực hiện những phần cứng VPN được tích hợp chỉ trong một thiết bị duy nhất nhưng vẫn đáp ứng được những chức năng cho VPN đang dần dần thay thế các nhu cầu thêm vào tường lửa hoặc bộ định tuyến đang tồn tại những phần mềm hay phần cứng, kể cả phần cứng cho các liên kết WAN trong một số trường hợp (xem hình 11.1).

Một trong những mục đích của những sản phẩm trong VPN là để ngưng tải (offload) những chức năng của VPN từ một tường lửa hay một bộ định tuyến không có đủ công suất tính toán để điều khiển các chức năng như mã hoá. Nhiều hệ thống được đề cập trong chương này tận dụng các ASIC đã được thiết kế chuyên dụng và trong một số trường hợp, sẽ sử dụng đến các vi mạch (chip) mã hoá đặc biệt nhằm cải thiện hiệu suất cho các hệ thống này.



Hình 11.1: Tích hợp các tính năng cho VPN

Không phải toàn bộ các sản phẩm được đề cập trong chương này đều thực hiện những tính năng giống nhau. Một vài sản phẩm hướng đến việc cung cấp giải pháp chìa khoá trao tay (turnkey solution) cho việc bảo mật, gồm cả tường lửa. Những phần cứng VPN khác trong phạm vi từ các gói sản phẩm cho đến các hệ thống trọn gói điều khiển mọi mặt của một kết nối Internet, bao gồm những kết nối WAN, việc định tuyến, các VPN, DNS và các dịch vụ về thư điện tử, cũng như một số dịch vụ khác...

11.1 Các loại phần cứng VPN

Một trong những điểm khác nhau giữa các sản phẩm thông dụng hiện nay chính là ở thiết bị khởi tạo đường hầm. Một cổng nối bảo mật có thể tạo ra một đường hầm để liên kết với LAN phục vụ đến một cổng nối khác, hoặc chỉ một host đầu xa có thể tạo ra một đường hầm để kết nối một cổng nối và LAN mà nó phục vụ. Chúng ta gọi đó là những VPN kết nối LAN-LAN hoặc là những VPN quay số. Chúng ta sẽ dùng thuật ngữ cổng nối VPN để mô tả những sản phẩm có thể điều khiển những VPN kết nối LAN-LAN, các trường hợp khác, ta sẽ dùng thuật ngữ truy cập từ xa.

Đánh giá về việc tích hợp

Việc tích hợp các chức năng khác nhau thành một sản phẩm duy nhất có thể có sức lôi cuốn đặc biệt đối với các khách hàng không đủ tài nguyên để cài đặt và quản lý một số các thiết bị mạng khác nhau và cũng không muốn đưa ra ngoài các hoạt động VPN của họ. Cài đặt một đường hầm có thể khiến cho việc thiết lập một VPN trở nên dễ dàng hơn việc cài đặt phần mềm trên một tường lửa và

cấu hình một bộ định tuyến, ví dụ như cài đặt một máy chủ RADIUS. Dĩ nhiên, điều này cũng như một phần mềm cấu hình cho một thiết bị VPN tích hợp.

Nói riêng về những khác biệt giữa các VPN kết nối LAN-LAN và những VPN quay số, một số nhà cung cấp có hai cách nhìn khác nhau về việc phát triển các thiết bị VPN tích hợp. Đối với một vài nhà cung cấp, một thiết bị tích hợp là một vị trí lý tưởng đối với việc bổ sung bất kỳ dịch vụ mạng nào khác để cho các người dùng có thể truy cập từ một vị trí nào khác. Do đó, họ đã gộp việc dùng các kỹ thuật như Web-caching, DNS caching, các máy chủ e-mail trong những thiết bị VPN của họ. Các nhà cung cấp khác thì xem các thiết bị VPN như một vị trí dành riêng cho việc điều khiển kết nối mạng, thực hiện việc quản lý băng thông và hạn chế tài nguyên.

Việc tích hợp nhiều chức năng vào một thiết bị duy nhất có thể tạo thành một thiết bị rất tốt, bởi vì thiết bị này bây giờ đã trở nên một điểm đơn khi có sự cố lỗi. Nó có thể thành một thiết bị chấp nhận mọi chức năng bảo mật trong quá trình điều khiển việc liên lạc với mạng Internet có khả năng xảy ra lỗi khi một thiết bị đơn bị hư, ít nhất, một tuyến thông tin bị phá vỡ bởi những kẻ phá hoại không thể truy cập vào mạng Intranet của ta thông qua liên kết trên. Nhưng nếu như các máy trên toàn bộ mạng của ta đang thực hiện việc gửi hay nhận e-mail khi tuyến liên kết trên bị bẻ gãy thì tất cả những dữ liệu của ta sẽ mất sạch.

Một trong những vấn đề lớn nhất đối với tất cả các thiết bị này là thiếu hỗ trợ trong việc đồng bộ hoá. Thật khó tìm được một nhà cung cấp thiết bị VPN có thể đáp ứng được toàn bộ các yêu cầu cho mọi vị trí trong VPN của chúng ta: công ty, các văn phòng chi nhánh, các vùng. Do việc đồng bộ hoá trở nên rất quan trọng khi ta quyết định mua các thiết bị khác nhau (của các nhà cung cấp khác nhau) cho những vị trí khác nhau trong VPN.

Sau đây chúng ta sẽ đề cập đến những sản phẩm khác nhau sẽ được sử dụng cho những VPN khác nhau như thế nào.

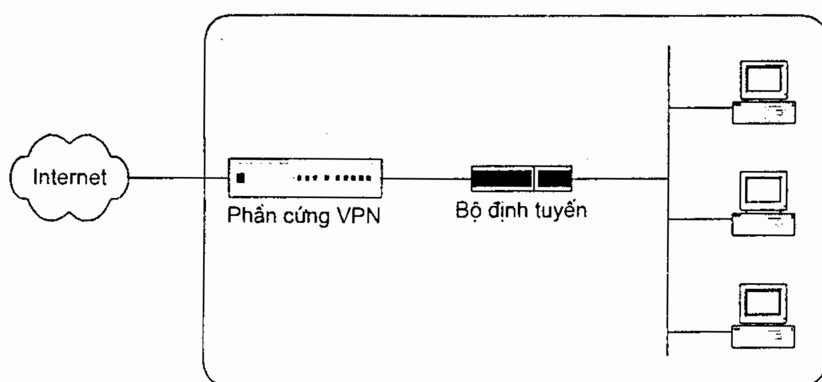
11.2 Áp dụng và cấu hình các sản phẩm phần cứng VPN

Ta đã biết những chức năng quan trọng mà bất cứ VPN nào cũng phải có đó là: định đường hầm, mã hoá, xác thực và quản lý khoa. Tùy thuộc vào việc quyết định sử dụng những giao thức nào cho VPN (như PPTP, L2TP, IPSec) mà những giao thức này sẽ có tầm quan trọng tương đối khác nhau với những chức năng trên. Ví dụ, PPTP thực sự là giao thức mạnh trong việc định đường hầm, nhưng nó lại yếu kém trong việc mã hoá, L2TP hỗ trợ xác thực người dùng mạnh hơn, IPSec lại có thế mạnh trong việc mã hoá. Nói cách khác, IPSec điều khiển việc mã hoá và quản lý khoá tốt nhưng giao thức này cần được hoàn thiện hơn để có

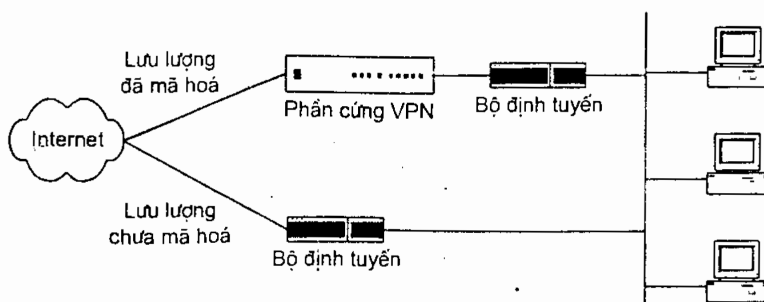
thể sử dụng được như một giao thức xác thực người dùng tốt. Như vậy, mỗi giao thức đều có những ưu điểm và nhược điểm riêng của mình.

Tùy thuộc vào các đặc điểm của sản phẩm mà các cổng nối có thể được đặt chung với các thiết bị VPN khác đã tồn tại trên mạng, cũng giống như tường lửa, hoặc chúng có thể được triển khai như các thiết bị mở rộng. Nói cách khác, nơi ta đặt cổng nối không những ảnh hưởng đến quyền thâm nhập và quyền ra vào mạng mà còn ảnh hưởng đến lưu lượng trên mạng. Mặc dù một cổng nối VPN có thể được tích hợp một số chức năng tốt khiến cho việc quản trị mạng trở nên đơn giản hơn, thì việc cài đặt một cổng nối có thể khiến ta phải thực hiện cấu hình lại những thiết bị hiện có trên mạng, chẳng hạn như các bộ định tuyến và tường lửa.

Nếu một cổng nối VPN có kèm theo một cổng giao tiếp WAN thì chúng ta có thể cài đặt nó theo 2 cách. Cách thứ nhất là đặt cổng nối này giữa kết nối của ISP và mạng Intranet của mình (xem hình 11.2).



Hình 11.2: Minh hoạ việc đặt cổng nối trước

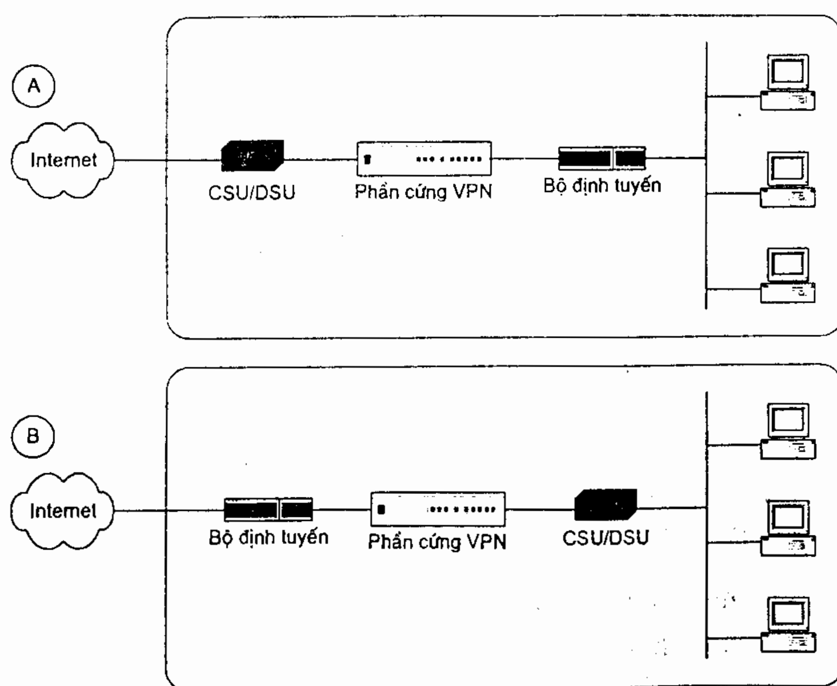


Hình 11.3: Các tuyến không mã hoá và mã hoá song song

Trong trường hợp cổng nối được đặt như thế này, cổng nối sẽ xử lý tất cả lưu lượng đến mạng và đi ra khỏi mạng. Cách sắp đặt như thế này là giảm thiểu yêu

cầu phải cấu hình lại cho bất kỳ thiết bị nào đang có trên mạng do cổng nối sẽ cung cấp những dịch vụ mã hoá và giải mã trong suốt cho toàn bộ địa điểm này và những bộ định tuyến và tường lửa hiện có trên mạng sẽ nhìn nhận các gói TCP/IP một các bình thường.

Nếu ta muốn mã hoá tất cả các lưu lượng gửi đến Internet, thì cách đặt cổng nối như trên sẽ không gặp bất cứ vấn đề nào, nhưng nếu xét một khía cạnh khác, nếu ta chỉ muốn mã hoá một số lưu lượng của một số ứng dụng (như e-mail, FTP) mà không muốn mã hoá lưu lượng của các ứng dụng khác (như Web, Telnet chẳng hạn) thì ta phải đảm bảo rằng sản phẩm phải thực hiện việc điều khiển ứng dụng chỉ định thông qua việc mã hoá, nếu không ta sẽ phải thiết lập hai kết nối khác nhau đến Internet: một kết nối dùng cho lưu lượng đã mã hoá và kết nối còn lại dùng cho lưu lượng chưa mã hoá (xem hình 11.3).



Hình 11.4: Các cấu hình cổng nối-bộ định tuyến khác

Cấu hình thứ hai cho các cổng nối VPN hỗ trợ WAN phải được bảo dưỡng một cách đặc biệt, bởi vì ta sử dụng đến hai thiết bị truy cập: ví dụ như một cổng nối VPN dành cho lưu lượng đã mã hoá và một bộ định tuyến cho lưu lượng chưa mã hoá. Và những thiết bị này phải chứa những quyền để đảm bảo những lưu lượng trên được chuyển đi một cách trực tiếp và thông qua thiết bị tương ứng.

Khi cổng nối VPN của ta không có cổng ra WAN mà chỉ có hai cổng Ethernet (hay nhiều hơn), lúc đó ta lưu ý đến 3 điểm khác nhau trong việc cấu hình là:

- Đặt cổng nối giữa một thiết bị truy cập và một thiết bị điều khiển truy cập (chẳng hạn như bộ định tuyến) với phần còn lại của LAN (xem hình 11.4A).
- Đặt cổng nối trước thiết bị truy cập (xem hình 11.4B).
- Hoặc cổng nối VPN đóng vai trò như một nút khác của LAN (hình 11.5).

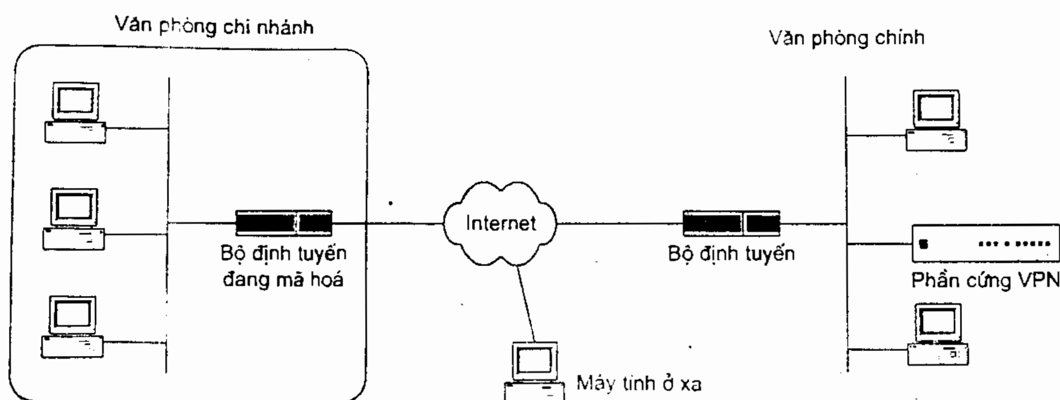
Trong trường hợp đầu, chúng ta điều khiển toàn bộ lưu lượng. Nếu ta đặt cổng nối giữa Internet và bộ định tuyến thì bộ định tuyến có thể được dùng để lọc cả hai lưu lượng VPN đã mã hoá và cả chưa mã hoá với cùng các quyền ưu tiên như nhau. Ngoài ra, chúng ta cũng không cần phải cấu hình lại để chuyển những lưu lượng đặc biệt trong trường hợp cổng nối được cài trước bộ định tuyến. Nhưng ta phải lưu ý đến một điều là nếu như cổng nối đặt trong mặt phẳng mạng công cộng, không có độ tin cậy, ta cần phải đảm bảo việc quản lý nó không thể bị một cá nhân nào đó trong mạng này làm tổn hại. Nếu liên kết trên đang điều khiển cả hai lưu lượng VPN và không-VPN thì cổng nối VPN cần phải được cấu hình để chuyển lưu lượng không-VPN.

Khi ta đặt cổng nối sau một thiết bị điều khiển truy cập thì thiết bị này phải được cấu hình để chuyển lưu lượng VPN mà không cần thực hiện việc lọc. Mặc dù kiểu cấu hình này tăng độ bảo mật cho cổng nối (tức nó giảm thiểu khả năng việc quản lý cổng bị tổn hại), ngoài ra việc cấu hình kiểu này còn làm cho ta ít phải điều khiển lưu lượng đưa vào LAN sau khi được giải mã bởi cổng nối. Nếu ta muốn lọc lưu lượng VPN thông qua đích đến của nó, theo giờ trong ngày hay theo loại ứng dụng thì ta phải sử dụng số bộ lọc gấp đôi hoặc là sử dụng việc cấu hình như trong hình 11.4B.

Việc cài đặt cổng nối VPN như một nút khác của LAN thường được gọi là cấu hình một nhánh (xem hình 11.5), cấu hình này có ảnh hưởng đến toàn bộ lưu lượng VPN theo 2 bước:

- Đến cổng nối để xử lý.
- Sau khi được xử lý xong, những lưu lượng này sẽ ra khỏi cổng nối để đến LAN.

Chúng ta cũng không cần quan tâm thêm về lưu lượng đến mạng ở các cấu hình trên, bởi vì cấu hình này cho phép việc cân bằng tải tối ưu (nhất là khi ta có nhiều liên kết đến Internet) và thực sự hữu ích khi ta phải điều khiển hàng trăm hay hàng ngàn phiên truyền cùng lúc với các khách hàng đầu xa.



Hình 11.5: Minh hoạ cấu trúc một nhánh

Đối với nhiều hệ thống, đặc biệt là những hệ thống dùng IPSec, các khoá phải được tạo cho những phiên làm việc và được kiểm tra xem chúng có hợp lệ hay không, điều này khiến cho phát sinh một số yêu cầu về quyền chứng nhận điện tử CA (Ceritificate Authority). Trong những hệ thống sử dụng các cặp khoá công cộng (public key pairs), các khoá riêng thường được tạo ra trong VPN và được lưu trữ trong bộ nhớ của các thiết bị. Điều này được thực hiện một cách tự động bằng một trong hai cách: hoặc là các khoá được phân phát đến mỗi thiết bị trong VPN (cách này hợp lý khi mạng có ít thiết bị) hoặc các khoá công cộng có thể được lưu trữ trong một danh mục trung tâm, chẳng hạn như một máy chủ chứng nhận.

Nếu ta có và phải quản lý nhiều khoá cũng như nhiều chứng nhận điện tử (digital certificates) thì nếu muốn, chúng ta có thể liên hệ những công ty chuyên đảm trách công việc này để họ giúp đỡ, một số công ty đó là CyberTrust, VeriSign.

Điểm quan trọng cuối cùng của VPN mà ta đã có dịp liệt kê đó là vấn đề xác thực (authentication), đối với nhiều nhà quản lý mạng thì việc xác thực và điều khiển truy cập hoàn toàn không phải là việc mới lạ gì, nếu như công ty của chúng ta đã sẵn sàng hỗ trợ các người dùng từ xa thông qua việc kết nối quay số bằng modem thì ta cần phải sử dụng một số hệ thống xác thực. Để tích hợp VPN vào liên mạng sẵn có của mình, chúng ta cần xem xét đến việc liên kết giữa các thiết bị này có tốt hay không, nhất là đối với các thiết bị dùng để xác thực và điều khiển truy cập.

Ta cũng cần biết thêm là mặc dù ngày nay nhiều sản phẩm có thể sử dụng RADIUS cho việc xác thực người dùng như RADIUS client, nhưng có một số ít

sản phẩm, như Extranet Switch - của hãng cung cấp thiết bị mạng Bay Network - đã từng bước kèm theo cả máy chủ RADIUS như một phần của sản phẩm.

Để thêm vào tính năng truy cập từ xa cho VPN, ta chỉ cần một phần mềm client do nhà sản xuất cổng nối cung cấp và cài đặt phần mềm client trên các máy ở xa này. Nếu ta đang tạo ra một VPN lai ghép thì nên nhớ tính toán số lượng người dùng từ xa có thể có khi xác định cổng nối của mình cần phải hỗ trợ bao nhiêu kênh cùng lúc.

Những yêu cầu đối với sản phẩm

Nếu như ta dự định sử dụng những thiết bị phần cứng như trong chương này đã đề cập đến như một cổng nối bảo mật cho chính VPN của mình, chúng ta cần phải quan tâm đến một số vấn đề có liên quan sau:

Trước hết, phải xác định là ta chỉ truyền những lưu lượng IP thông qua VPN hay là ngoài ra sẽ hỗ trợ cả IPX và NETBEUI? Có nhiều cổng nối chỉ hỗ trợ IP, điều này tốt đối với những mạng sử dụng IP, nhưng chúng sẽ không giúp ích gì cho ta nếu mạng của ta đang chạy Netware thông qua IPX chẳng hạn. Nếu ta không muốn chọn việc chuyển Netware thành phiên bản hỗ trợ cho IP, hay không muốn sử dụng cổng nối IPX-IP, hoặc không muốn thay thế Netware hiện có để tạo ra những mạng chỉ dùng IP thì ta phải sử dụng cổng nối hỗ trợ PPTP hoặc L2TP để có thể điều khiển cùng lúc nhiều giao thức như trên.

Bất kể ta sử dụng giao thức nào cho VPN của mình thì ta cũng phải quan tâm đến việc sản phẩm được tích hợp với hệ thống bảo mật và hệ thống quản lý mạng như thế nào. Ví dụ, nhiều hệ thống phụ thuộc vào RADIUS hay các hệ thống dựa trên thẻ đối với việc xác thực. Nếu chúng ta sẵn sàng sử dụng một hệ thống riêng cho việc xác thực các người dùng từ xa thì hãy chọn một cổng nối tương thích với hệ thống xác thực hiện tại để nhằm đơn giản hoá việc cấu hình và quản lý các cổng nối.

Chúng ta nên kiểm tra những giải thuật mã hoá mà sản phẩm hỗ trợ, giải thuật mặc định là IPSec, giải thuật DES CBC dành cho việc mã hoá và giải thuật trộn HMAC-MD5 hoặc HMAC-SHA-1 dành cho việc xác thực, những giải thuật này đáp ứng các yêu cầu mà ta đã đề cập với lưu lượng có mức rủi ro trung bình, nếu như lưu lượng của chúng ta có mức rủi ro cao hơn, chúng ta phải kiểm tra sản phẩm phần cứng trên có hỗ trợ việc định khoá tự động hay không.

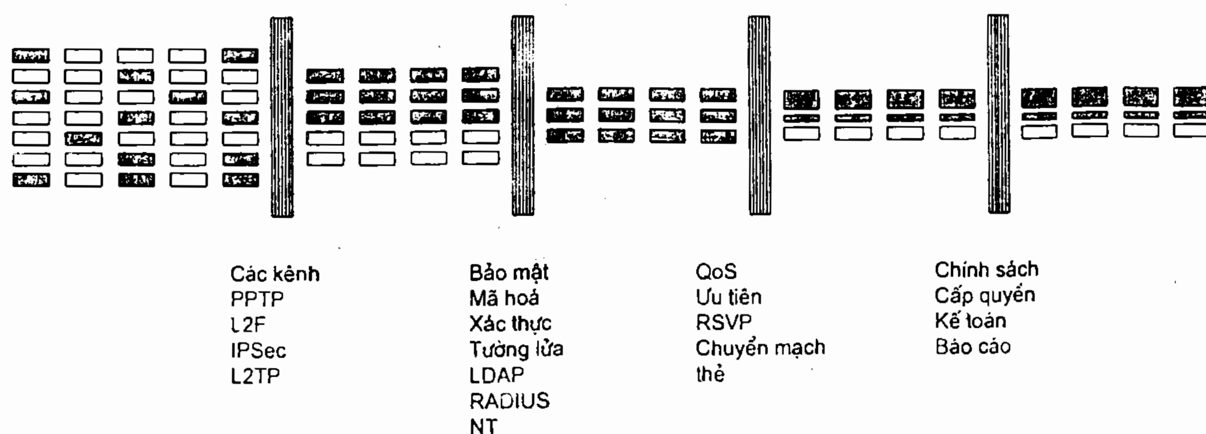
Phần lớn việc quản trị khoá không những phụ thuộc vào độ tin cậy và tính bảo mật của chứng nhận điện tử hay máy chủ chứng nhận mà nó còn phụ thuộc vào sự phản ứng của các sản phẩm như thế nào trong trường hợp một phần trong tiến trình quản trị khoá bị lỗi hay một khoá bị hủy bỏ. Một số sản phẩm sẽ ngừng (drop)

phiên làm việc ngay tức khắc khi phát hiện ra một khoá bị hủy một số sản phẩm khác sẽ chờ cho đến khi phiên làm việc hoàn thành. Ngoài ra, để cung cấp thêm khả năng sao lưu dự phòng đối với các khoá khi một CA bị lỗi, chúng ta phải định ra một thiết bị phần cứng lưu trữ các khoá dành riêng cho một cổng nối VPN.

11.3 Tổng quan về những sản phẩm phần cứng VPN

Đối với việc quản trị khoá, nhiều sản phẩm phụ thuộc vào máy chủ chứng nhận đã được cài đặt trên hệ điều hành Windows NT hay Unix. Một số phần cứng có tính năng bảo mật tốt như CIPro có thể được cài đặt cho việc quản trị khoá, cho phép VPN tiếp tục chạy thậm chí không cần có chứng nhận điện tử. Một số sản phẩm mà ta đã đề cập đến trong phần này có thể cho phép nhiều thiết bị hoạt động song song và một thiết bị có thể sẽ thực hiện chia tải với một thiết bị khác khi thiết bị đó bị hư, chẳng hạn như Extranet Switch của hãng Bay Network và LanRover cổng nối VPN của hãng Shiva có kèm theo những tính năng miễn lỗi.

Mặc dù có nhiều thiết bị cung cấp hiệu suất tối ưu cho VPN, nhưng ta cũng phải quyết định nên tích hợp bao nhiêu tính năng trong cùng một thiết bị duy nhất. Đối với những doanh nghiệp nhỏ hay những văn phòng nhỏ, không có số lượng nhân viên lớn, tốt nhất chúng ta tích hợp tất cả các tính năng của VPN trong cùng một sản phẩm như một tường lửa và có thể thêm một hay hai dịch vụ mạng khác. Một số sản phẩm - thường rất đắt tiền - gồm có cả các nguồn công suất đôi và những tính năng miễn lỗi. Tuy nhiên, chúng ta cần phải quyết định dịch vụ mạng nào là có tính quyết định đối với hoạt động thường xuyên của công ty, để sau đó định mức ưu tiên cho các dịch vụ và có thể chúng ta sẽ quyết định khi nào thì sẽ cài đặt chúng trong cùng một sản phẩm duy nhất.



Hình 11.6: Tích hợp VPN và QoS

Ngoài ra, chúng ta không nên bỏ qua đặc điểm quan trọng việc tích hợp các chức năng điều khiển liên quan đến mạng, như việc cấp phát tài nguyên và việc điều khiển băng thông. Ta có thể xem hình 11.6 để hiểu rõ hơn.

Bảng 11.1: Tham khảo một số cổng nối VPN thông dụng

	1	2	3	4	5	6
Sản phẩm (Công ty)	Adi (Assured Digital)	Cipro-vpn (Radguard)	Lanrover vpn gateway (Shiva)	Permit connect (Timestep)	Safenet lan (IRE)	Secure domain (Cylink)
Giá	Adi-500: $995 Adi-1000: $12954 Adi-2000: $1595 Adi-4500: $20000	$ 6450	$9250	$7995 (chia sẻ bí mật). $14395 (giao cho PKI)	$4995	$3500
Phần mềm truy cập từ xa	Win95	Win95, NT (Unix)	Win95, NT	Win95, NT	Win3.11, 95, NT	Win3.x, 95, NT
Giao thức định đường hầm	IPSec, PPTP	IPSec	IPSec	IPSec	IPSec và độc quyền	Độc quyền
Giao thức được hỗ trợ	TP/IPX	TCP/IP	TCP, IP	IP, IPX	IP	IP, IPX
Kiểu mã hoá	DES, Triple DES, IPSec	DES, RSA, MD5	DES, Triple DES	IPSec, DES	IPSec, (ESP), DES	DES, độc quyền
Xác thực gói	MD5, SHA-1	IPSec AH	RSA SOURCE	MD5, RSA	IPSec AH	MD5, SHA-1
Điều khiển truy cập		Nguồn, đích, ứng dụng, toàn thời gian (suốt ngày)	Đích, cổng, địa chỉ IP, đoạn LAN	Đoạn LAN	Nguồn, đích, địa chỉ IP, cổng, giao thức	

	1	2	3	4	5	6
Xác thực người dùng		X.509 securenet	Miền người dùng NT, RADIUS, Secure ID, X.509	X.509, miền người dùng NT	ANSI X9.26, mật khẩu dùng một lần	
Quản lý khoá	IKE	IKE	IKE	RSA, độc quyền	ANSI X9.17 IKE	Diffie-Hellman
Các đường hầm được hỗ trợ	1000 quay số hoặc 400 tốc độ cao (tối đa cho ADI-4500)		1024	200		
Các nút được hỗ trợ			Không giới hạn	50004		
Tích hợp tường lửa	Không	Có	Có	Có	Có	Không
Loại tường lửa		Lọc gói, proxy ứng dụng	Proxy ứng dụng, lọc gói		Lọc gói, proxy	Không có
Quản trị từ xa			Có	Có	Có	
Các chứng nhận	X.509	X.509	X.509	X.509		Có
Client truy cập từ xa	Có	Không	Có	Có	Có	Không
Phần mềm quản trị		HP Open View (Win95)	Win95, NT	Win NT,95	Win	Win
Nén		Không	Không	Không	Không	
Tái định khoá		Tự động	Tự động		Tự động	
Các cổng WAN	Thay đổi theo kiểu	Không				
NAT		Có	Có			Có

	1	2	3	4	5	6
Các chức năng khác	ADI-2000 gồm 8 cổng Ethernet hub; ADI-500 = card PCI cho máy chủ	Giám sát lưu lượng, nhật ký sự kiện, chứng nhận điện tử; phục hồi cấu hình VPN	Cân bằng tải, dự phòng giữa các khối phức tạp			
Các sản phẩm khác		Máy chủ chứng nhận $6500	Quản trị CA chuyển mạch ($2400)	PERMIT/Gate 2520 IPSec 2-cổng dùng cho cổng nối (4Mbit/s). PERMIT/Gate IPSec 2-cổng dùng cho cổng nối (10Mbit/s)	SafeNet/ Secure Center (chuyển mạch và trạm làm việc) $15995; SafeNet/Soft (host-host IPSec chuyển mạch) $79; SafeNet/ Smart (smartcard và bộ đọc), $1254	Phần mềm quản trị, $10000

Bảng 11.2: Một số sản phẩm cổng nối VPN từ xa thông dụng

	1	2	3	4
Sản phẩm (công ty)	Extendnet VPN (Extended Systems)	Contivity Extranet switch (BAY Networks)	Intraport VPN access server (Compatible Systems)	Riverworks (Indus River)
Giá	$2999 (10 đầu nối); $5999 (25 đầu nối); $9999 (50 đầu nối)	ES1000: $2000 ES2000: $20000 ES4000: $50000	Intraport 2: $3995 Intraport 24: $9995 Intraport Enterprise: $35000	$25000
Phần mềm truy cập từ xa	Win95, NT	Win95, NT	Win95, NT, Mac, Linux, GRE, IPSec	Win95, NT

	1	2	3	4
Giao thức định đường hầm	PPTP	PPTP, L2F, L2TP, IPSec		PPTP, IPSec
Các giao thức được hỗ trợ	IP, IPX	TCP/IP, IPX	IP, IPX	IP, IPX
Kiểu mã hoá	MPPE	DES, Triple DES, RC4	STEP, MD5, IPSec, DES, Triple DES	IPSec, DES, Triple DES
Xác thực gói	PPTP	IPSec AH	IPSec AH, MD5, SAH nguồn, đích.	PPTP
Điều khiển truy cập		Nguồn, đích, địa chỉ IP, cổng, dịch vụ, người dùng	Địa chỉ IP, cổng, dịch vụ, người dùng	
Nhận dạng người dùng	CHAP, MSCHAP, PAP, RADIUS, miền người dùng NT	RADIUS LDAP, miền người dùng NT, Axent, Secur ID, LDAP	RADIUS	CHAP, RADIUS, SecurID
Quản lý khoá	MS RAS chia sẻ bí mật	IKE	Diffie-Hellman	
Hỗ trợ nút	Không giới hạn	Không giới hạn	Không giới hạn	Không giới hạn
Tích hợp tường lửa	Tuỳ chọn	Có	Có	Không
Các đường hầm được hỗ trợ	50	ES1000: 50 ES2000: 200 ES4000: 2000	Intraport 2: 64 bộ kết nối từ xa, 16 bộ kết nối site-site; Intraport 24: 200 bộ kết nối từ xa, 32 bộ kết nối site-site; Intraport Enterprise: 2000 bộ kết nối từ xa, 64 bộ kết nối site-site	2000
Loại tường lửa		Lọc gói	Bộ lọc gói bị giới hạn	
Quản trị từ xa	Có	Có	Có	Có
Các chứng nhận	Không	X.509	Không	Không
Client truy cập từ xa	Có	Có	Có	Có

	1	2	3	4
Phần mềm quản trị	Win	Win	Win	Win
Nén	Có (MPPC)	Không		Có
Tái định khoá	Có	Có	Có	Không
Các chức năng khác		Quản trị băng thông, LDAP		Máy chủ truy cập từ xa
Các cổng WAN	Không	Tuỳ chọn		T1, T3
NAT	Không	Có	Không	Không

Một số công ty đã kèm những đặc điểm trên vào những sản phẩm của họ và trong tương lai những sản phẩm này sẽ hỗ trợ cho một số tính năng khác. Việc tích hợp điều khiển lưu lượng với xác thực làm cho việc quản lý mạng dựa trên chính sách trở nên hữu ích và phổ biến.

Trong bảng 11.2, chúng ta sẽ tham khảo một số sản phẩm phần cứng và các giá cả trong bảng này chỉ có giá trị tham khảo, nếu muốn biết thêm các chi tiết cụ thể của sản phẩm, ta phải liên hệ trực tiếp hoặc thông qua các trang Web của các nhà sản xuất.

TỔNG KẾT

Nếu chúng ta quan tâm đến vấn đề hiệu suất thì ta nên chọn các sản phẩm phần cứng VPN thay cho các sản phẩm phần mềm (do phần cứng thực hiện việc mã hoá, giải mã nhanh hơn nhiều so với phần mềm). Đa số các thế hệ hiện tại của những sản phẩm phần cứng này bao gồm xác thực gói, định đường hầm, mã hoá và quản lý khoá cũng như các liên kết đến hệ thống xác thực người dùng. Nhiều sản phẩm còn hỗ trợ trọn gói nhiều dịch vụ trong cùng một thiết bị, chẳng hạn như máy chủ RADIUS và LDAP và hỗ trợ đồng thời hàng ngàn kênh truyền.

CHƯƠNG 12

PHẦN MỀM CHO VPN

Như trong chương trước ta đã đề cập đến những vấn đề căn bản về phần cứng cho VPN, trong chương này chúng ta sẽ đề cập đến nhóm sản phẩm cuối cùng đó là những sản phẩm phần mềm dùng cho VPN. Dĩ nhiên chúng ta không thể nào giới thiệu hết những sản phẩm phần mềm được (do ngày nay, nền công nghiệp phần mềm phát triển rất mạnh và có nhiều công ty phần mềm đưa ra những sản phẩm của họ về VPN), chúng ta sẽ giới thiệu những đặc điểm, yêu cầu chung mà chúng cung cấp và đề cập chủ yếu đến những phần mềm hệ điều hành chính (NOS) như Windows NT của Microsoft, Novell của Netware. Các phần mềm này được dùng để định dạng và quản trị các kênh bảo mật, ngoài ra chúng cũng có thể được sử dụng cho các kênh giữa các host mà không cần sử dụng đến cổng nối bảo mật.

12.1 Các sản phẩm phần mềm dùng cho các loại VPN khác nhau

Chúng ta sẽ đề cập đến hai lớp phần mềm: các phần mềm của lớp 1 được dùng để cung cấp các dịch vụ VPN cho một mạng LAN, mục đích của chúng cũng giống như của các thiết bị phần cứng mà ta đã đề cập chương trước; lớp 2 bao gồm những phần mềm dùng cho việc định đường hầm giữa các host mà không cần dùng đến một cổng nối bảo mật.

Các sản phẩm cung cấp những dịch vụ VPN cho mạng LAN thực hiện đầy đủ toàn bộ việc định đường hầm và các kế hoạch của VPN, một số sản phẩm này hỗ trợ cả những giao thức PPTP, L2TP mà ta đã có dịp nói đến ở những chương trước. Một số khác sử dụng những kế hoạch thích hợp để định đường hầm và quản lý khoá.

Ngày nay, sự phát triển của các chuẩn về VPN, những nền tảng thiết yếu cho chúng (ví dụ như chứng nhận điện tử) và thị trường mạng hiện đại đã khiến

cho những giải pháp về LAN có mức độ ưu tiên hơn so với các giải pháp liên lạc giữa các host.

Mặc dù một số ít sản phẩm cục bộ có thể được sử dụng trong việc bảo mật các kết nối host-host, nhưng đa số các nhà thiết kế đã sử dụng những công cụ phát triển phần mềm SDK (Software Development Kit) có tính thương mại để tạo ra những chương trình tương thích với IPSec. Điều này cũng dễ hiểu là các nhà lập trình đa số đều muốn phần mềm của mình phù hợp với thị hiếu sử dụng của khách hàng.

12.1.1 Các phần mềm định đường hầm

Về thực chất, việc định đường hầm cũng không có gì khác biệc với việc bọc gói, trong một số trường hợp, chẳng hạn như Mbone, dựa trên thực nghiệm qua việc quảng bá trên mạng đường trục Internetđã chỉ ra rằng: việc bảo mật một gói đã được đóng gói là không đạt kết quả, ví dụ như với PPTP rốt cục việc bảo mật cũng không mang lại kết quả gì khả quan hơn, lý do tại bản thân các phương pháp này không cung cấp phương pháp bảo mật hiệu quả.

Với phần mềm cho VPN, chúng ta có thể thấy rằng việc đóng gói để định dạng kênh có thể thực hiện theo những phương pháp khác nhau. Trong chương này, chúng ta sẽ đề cập đến các phương pháp dùng cho việc định đường hầm và lưu ý rằng mỗi phương pháp đều không tương thích với các phương pháp còn lại.

Chúng ta đã nói khá nhiều về các chuẩn và các sản phẩm hỗ trợ liên điều khiển, cũng như ta từng xem xét IPSec. Quyền được tự do chọn lựa và lựa chọn nhiều nhà cung cấp cho phép chúng ta mua được những sản phẩm tốt nhất cần thiết mà không phải ràng buộc với một nhà cung cấp nào - tức là chúng ta có thể có những sản phẩm tốt nhất từ nhiều nhà cung cấp vì thường một nhà cung cấp sẽ có một thế mạnh nào đó. Dĩ nhiên, chúng ta vẫn phải lo lắng trong việc cấu hình và quản lý những thiết bị khác nhau nếu ta mua chúng từ nhiều nhà cung cấp. Các doanh nghiệp thường chọn mua những sản phẩm của cùng một nhà cung cấp để tránh những khó khăn trong việc quản lý và bảo dưỡng.

Do thị trường phần mềm có sự cạnh tranh mạnh nên các nhà sản xuất phải thường xuyên thay đổi, nâng cấp các sản phẩm của mình để đưa ra những sản phẩm có khả năng cạnh tranh mạnh, do đó người dùng sẽ được nhiều lợi ích hơn. Chẳng hạn như hai nhà sản xuất Alta Vista Tunnel và Borderguard từ lâu đã dự định kèm theo hỗ trợ IPSec trong sản phẩm của họ.

Chúng ta có thể không cần dùng đến IPSec và L2TP mới có thể tạo ra VPN cho mình, ta có thể dùng các giao thức khác, ví dụ như SOCKS v5 hay Secure Sheil (SSH) của Datafellows trong các sản phẩm F-secure. SSH là giao thức quen thuộc của những nhà quản trị hệ điều hành Unix trong việc bảo mật thông tin liên

lạc và được sử dụng trong một số mạng khác (ví dụ như mạng của NASA hay mạng của các ngân hàng) để việc truyền số liệu được bảo mật. Tuy nhiên, ta nên lưu ý rằng không giống như các giao thức mà ta đã đề cập, SSH hoạt động ở lớp giao vận trong mô hình OSI.

12.1.2 VPN và các sản phẩm dựa trên hệ điều hành mạng

Trước khi đề cập đến các sản phẩm VPN hoạt động dựa trên hệ điều hành mạng (NOS), chúng ta đề cập sơ qua về việc xây dựng một hệ điều hành mạng. Nói chung có hai cách để xây dựng một hệ điều hành mạng đó là:

Cách 1: Xây dựng một hệ điều hành mạng như tập hợp các tiện ích chạy trên một hệ điều hành sẵn có (ví dụ như Netware của hãng Novell).

Cách 2: Xây dựng một hệ điều hành mạng độc lập, tự thực hiện tất cả các công việc của một hệ điều hành thông thường kèm theo những chức năng hỗ trợ mạng (ví dụ như Windows NT của hãng Microsoft, Unix Linux).

Cách 1 có ưu điểm là dễ xây dựng, gọn nhẹ tuy nhiên không có tính hệ điều hành một cách đúng nghĩa và dĩ nhiên không tối ưu so với cách 2 (tuy cách 2 có khó khăn hơn trong việc thực hiện)

Trở lại với vấn đề mà chúng ta đang muốn đề cập: VPN và các sản phẩm dựa trên hệ điều hành mạng (NOS), mặc dù ngày nay các chức năng xác thực và mã hoá đã được gộp vào như một thành phần của hệ điều hành mạng, nhưng chúng ta vẫn phải tập trung trong việc sử dụng các cổng nối bảo mật hoặc các phần mềm client đầu xa khi muốn tạo ra các VPN. Từ lúc bắt đầu cung cấp hệ điều hành mạng có hỗ trợ cho VPN, những công ty như Microsoft hay Novell đã cung cấp những tính năng cổng nối bảo mật trong các phần mềm hệ điều hành mạng của họ.

Chúng ta nên biết là Micorsoft là hãng đầu tiên cung cấp máy chủ định đường hầm cho PPTP trong máy chủ truy cập từ xa và định tuyến RRAS của họ (Routing and Remote Access Server). Đây là sản phẩm chạy trên hệ điều hành WindowsNT version 4. Mặc dù RRAS được thiết kế để phục vụ như một máy chủ định đường hầm cho PPTP (và cả L2TP), cho các liên kết kết nối LAN-LAN hay host-host, nhưng nó không kèm theo các dịch vụ bảo mật như các sản phẩm khác. Ví dụ, RRAS có một hệ thống lọc gói rất hạn chế - chúng ta chỉ có thể cho phép chuyển các gói PPTP hay là không chuyển bất kể gói nào. Để thêm tính bảo mật của một tường lửa dùng điều khiển truy cập, ta phải cài thêm máy chủ proxy vào trong máy tính làm chức năng tường lửa trên.

Ngoài Microsoft, còn có một hãng chuyên cung cấp hệ điều hành mạng đó là Novell. Tuy ngày nay, thị phần của Novell có ít hơn Microsoft, nhưng sản phẩm

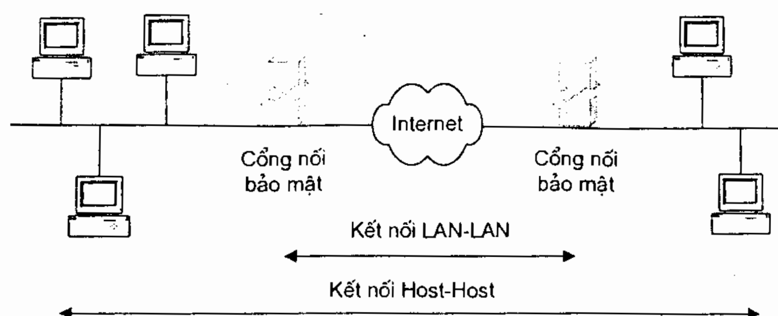
của hãng này vẫn còn được sử dụng một cách rộng rãi. Sản phẩm Borderguard của hãng Novell là một tập các mô đun phần mềm có thể sử dụng một cách độc lập hay dùng chung như một đơn vị (như ta đã giới thiệu ở trên, Novell dùng cách 1 trong việc xây dựng hệ điều hành mạng của mình). Và một trong những lý thú nhất của họ sản phẩm này là các mô đun cho tường lửa và VPN. Tường lửa hoàn toàn là một chương trình lọc gói chung và thuộc loại proxy ứng dụng. Các dịch vụ VPN của Borderguard sử dụng những công nghệ lọc gói của chính hãng Novell để mã hoá các gói TCP (sử dụng giải thuật mã hoá RC2). Ngoài ra, sản phẩm này còn sử dụng giao thức quản trị khoá đơn giản cho IP - SKIP (Simple Key Management for IP) để trao đổi các khoá, mặc dù điều hiển nhiên là việc thực hiện này không thể liên điều khiển với các máy chủ quản trị khoá của các nhà cung cấp khác Novell (do không cùng công nghệ).

Mặc dù Borderguard có thể không tương thích với hầu hết các VPN, nhưng nó là một sản phẩm lý tưởng cho nhiều công ty hiện đang sử dụng Netware và IPX, nhưng không muốn thiết lập một VPN. Do Borderguard có kèm theo một mô đun phần mềm làm chức năng tường lửa và nó có khả năng chuyển đổi IPX thành IP, chúng ta có thể thiết lập một VPN mà không cần chuyển đổi các mạng đang sử dụng giao thức IPX thành các mạng dùng IP, ta nên tiếp tục sử dụng Borderguard như một phần mềm VPN để chuyển đổi các thành phần của mạng từ IPX thành IP, do nó hỗ trợ cả hai giao thức IPX và IP. Tuy nhiên, do việc cài đặt Borderguard chỉ ảnh hưởng đến một phần VPN, chúng ta không thể chuyển những vị trí không dùng Netware thành VPN một các dễ dàng được.

Như vậy chúng ta có thể cài được bao nhiêu dịch vụ trên cùng duy nhất một máy tính? Câu trả lời liên quan đến hai vấn đề: thứ nhất là thông số điểm đơn của lỗi (single point of fairlure argument) mà ta đã từng đề cập đến trong chương trước, đó là câu hỏi: Có bao nhiêu dịch vụ mạng có khả năng bị mất mát dữ liệu nếu máy tính đơn trên bị hư? Vấn đề thứ hai liên quan đến hiệu suất: Việc chúng ta cài nhiều dịch vụ trên cùng một máy đơn duy nhất thì có ảnh hưởng như thế nào đối với hiệu suất mạng của những dịch vụ quan trọng. Điều này hiếm khi xảy ra đối với phần cứng VPN mà ta đã đề cập trong chương 11, bởi vì nhiều sản phẩm đã sử dụng những hệ điều hành và phần cứng tối ưu để nhằm đạt được hiệu suất cao nhất. Tuy nhiên, việc chạy một số các dịch vụ mạng khác trên cùng một máy đơn sử dụng một hệ điều hành đã được thiết kế cho một số các công việc khác thì sẽ không tối ưu đối với các dịch vụ mạng của mình (ví dụ: người ta thường khuyến nghị rằng không nên cài tất cả mô đun của Borderguard, nhất là mô đun Web caching trên cùng một máy tính duy nhất).

12.1.3 Các VPN liên host

Cả hai VPN kết nối LAN-LAN và host-host đều có liên quan đến một số loại cổng nối bảo mật. Nhưng một số loại VPN liên quan đến việc liên lạc giữa các host riêng biệt, các kết nối LAN-LAN VPN không yêu cầu dùng bất cứ cổng nối bảo mật nào để tạo ra các kênh hay các gói mã hoá bởi vì tất cả việc mã hoá thì được thực hiện trên các host (xem hình 12.1).



Hình 12.1: Các kết nối host-host và kết nối LAN-LAN

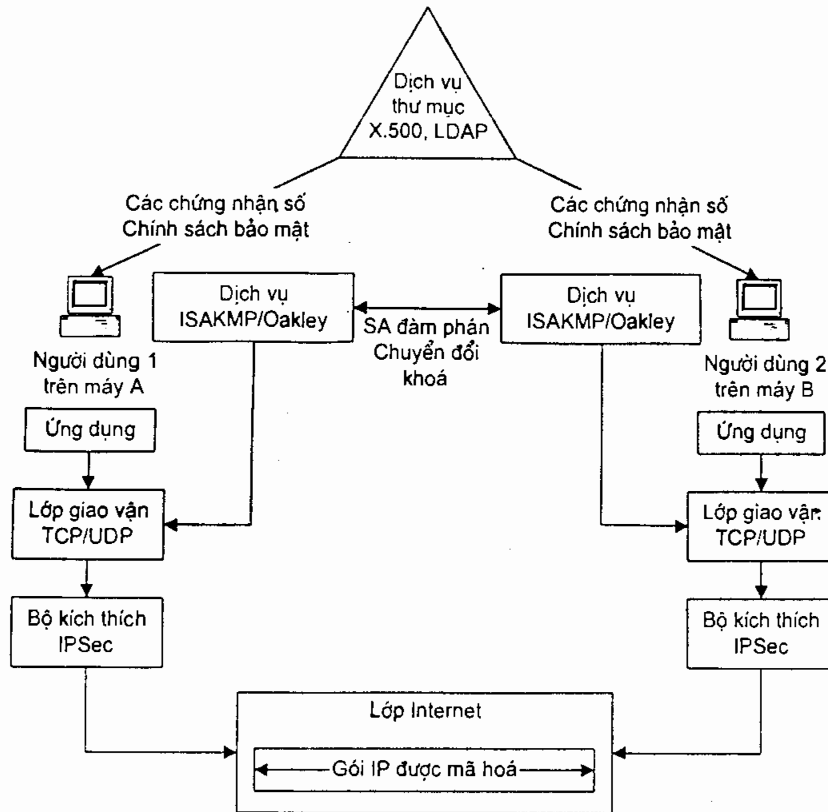
Mặc dù các chuẩn cho IPSec cung cấp các kết nối host-host, nhưng hiện nay các sản phẩm chính tương thích với IPSec chú trọng vào việc sử dụng một cổng nối bảo mật cho một số lý do khác. Thứ nhất, thị trường này vẫn còn mới mẻ và việc triển khai các phương tiện bảo mật tại ranh giới mạng (như bộ định tuyến, tường lửa và các cổng nối VPN) làm cho việc phát hiện các thay đổi trong VPN trở nên dễ dàng hơn. Lý do thứ hai là việc quản lý khoá thật sự sẽ dễ dàng hơn khi số lượng cổng nối có liên quan ít đi (mặc dù việc quản lý các khoá cho các host đầu xa sử dụng các VPN quay số có thể so sánh với việc quan tâm đến toàn bộ các host trên mạng). Lý do thứ ba là việc giảm hụt về hiệu suất do thực hiện việc mã hoá hay giải mã cho các gói có thể trở nên đáng kể khi mạng của chúng ta có nhiều máy tính và làm cho việc hoạt động của các máy trạm độc lập sẽ trở nên chậm đi nhiều trong khi thực hiện một chức năng cơ bản.

Tất cả nhân tố kể trên có thể làm chậm việc triển khai của việc mã hoá đồng thời trong các host độc lập, nhưng hiện tại người ta không thể không vượt qua các trở ngại trên để thiết lập các kết nối host-host VPN. Một số vấn đề khác cần lưu tâm là IPSec nguyên gốc được phát triển song song với thành tựu đạt được để định nghĩa phiên bản kế tiếp của IP là IPv6, điều này có nghĩa là tất cả các lớp giao thức của IPv6 và các trình điều khiển của nó đều bao hàm luôn IPSec và các chồng ứng dụng TCP/IP phải được hiệu chỉnh để có thể sử dụng được IPSec.

12.2 Các yêu cầu của sản phẩm

Khi chọn lựa phần mềm VPN cho một LAN, thì phần mềm này phải thỏa mãn nhiều yêu cầu khác nhau, nhưng ở đây chúng ta sẽ chỉ đề cập đến những yêu cầu chính như sau:

- Giao thức được hỗ trợ: đầu tiên, sản phẩm này hỗ trợ giao thức nào trong việc truyền thông qua mạng VPN của chúng ta: nó chỉ hỗ trợ IP hay hỗ trợ IPX và NETBEUI? Chẳng hạn như nhiều cổng nối chỉ hỗ trợ IPSec cho những mạng chỉ dùng IP, nhưng chúng sẽ không giúp ích gì được cho ta nếu mạng của ta đang chạy phần mềm Netware sử dụng giao thức IPX.
- Khả năng tích hợp với các hệ thống hiện có: chúng ta cần xem xét sản phẩm ta chọn tích hợp như thế nào đối với các hệ thống quản lý mạng và hệ thống bảo mật đang có trên mạng. Ví dụ, nhiều hệ thống lệ thuộc vào RADIUS hay các hệ thống dựa trên thẻ đối với việc xác thực người dùng, nếu chúng ta sẵn sàng sử dụng một hệ thống riêng để xác thực các người dùng đầu xa thì chọn một cổng nối tương thích với hệ thống xác thực hiện tại để đơn giản hoá việc cấu hình và quản lý các cổng nối.
- Việc cấp phát chứng nhận điện tử: Nếu ta dự định sử dụng một hệ thống xác thực dựa trên các chứng nhận điện tử thì ta phải nghĩ đến việc các chứng nhận điện tử này được phân phối và kiểm tra như thế nào, các vấn đề này sẽ được đề cập chi tiết hơn ở chương sau (chương 13: "Quản lý bảo mật"). Tuy nhiên, ở đây chúng ta nên xem xét một vài yếu tố như khi nào thì một chứng nhận điện tử được bảo dưỡng trong nội bộ mạng hay ở bên ngoài và các chứng nhận sẽ liên kết với các dịch vụ khác như thế nào? Một số thiết bị bao gồm cả các liên kết LDAP để có thể sử dụng với các máy chủ chứng nhận và trong một ít trường hợp, sẽ dùng chung với các máy chủ LDAP của chúng.
- Bảo dưỡng nhiều vị trí: ta nên lưu ý rằng khi chuẩn bị cài đặt các sản phẩm phần mềm tại nhiều vị trí trong VPN, có khả năng chúng ta phải bảo dưỡng một cơ chế bảo mật có tính hòa hợp cao hơn nếu sản phẩm ta đã chọn này có hỗ trợ việc quản trị đồng bộ cho nhiều vị trí. Điều này có thể liên quan đến việc trao đổi các tệp hay một vài dạng quản lý đầu xa (ví dụ như VTPC/secure, sẽ tạo một đĩa mềm chứa các tệp cấu hình cần thiết cho mỗi cổng nối để hoàn thành quá trình cài đặt phần mềm). Nếu sản phẩm có khả năng quản lý từ xa, ta phải đảm bảo việc truy cập từ xa đến các sản phẩm này phải có tính bảo mật.



Hình 12.2: Tương tác giữa các host và một máy chủ danh mục

- Giải thuật mật mã được hỗ trợ: chúng ta kiểm tra sản phẩm này hỗ trợ giải thuật mật mã nào, giải thuật mặc định IPSec, DESCBC dùng cho việc mã hoá và các giải thuật trộn HMAC-MD5 hay HMAC-SHA-1 cho việc xác thực người dùng, phải đáp ứng được với lưu lượng có độ rủi ro ở mức trung bình. Nếu lưu lượng của mạng có độ rủi ro cao, chúng ta phải chọn sản phẩm hỗ trợ việc tái định khoá tự động (automatic rekeying). Việc tái định khoá tự động làm tăng khả năng bảo mật cho mạng vì chúng sẽ gây nhiều khó khăn cho những kẻ tấn công trong việc sử dụng khoá đã lấy cắp (ví dụ khi kẻ tấn công lấy được một khoá thì khoá đó đã trở nên hết hạn sử dụng). Do vậy một số sản phẩm đã không dùng IPSec mà chỉ hỗ trợ một số thủ tục tái định khoá tự động. Phần mềm dùng cho việc thông tin liên lạc giữa các host phải hỗ trợ IPSec chế độ giao vận, mặc dù các cổng nối bảo mật thường chỉ cần dùng IPSec chế độ đường hầm là đủ. Do các tập hợp bảo mật có tính quyết định đến hoạt động của IPSec nên chúng ta có khả năng phải nhập thủ công các tập hợp bảo mật này (thường từ một tệp như theo khuyến nghị của S/WAN) và nếu có thể chúng ta phải định ra một tập bảo mật các ký tự liên kết. Để cung cấp tính thêm tính bảo mật

cho VPN, ta nên mua các sản phẩm của nhà cung cấp nào có hỗ trợ của hệ thống khử phát lại của IPSec phiên bản mới thay vì sử dụng một biến thể không được chuẩn hoá.

- Nhật ký ghi nhận xung đột: mỗi cổng nối bảo mật đều có một cách ghi nhận riêng các biến cố bảo mật và tường thuật lại chúng. Nếu có thể, chúng ta hãy đảm bảo hệ thống của mình phải khởi tạo được một số cảnh báo nếu một hoạt động nào đó chiếm chỗ thường trực.

Trong tương lai, ở phần mềm dựa trên host, IPSec chế độ giao vận sẽ được triển khai cho các máy tính độc lập, chúng giống như các máy chủ chứng nhận, có thể sử dụng LDAP, ngoài ra chúng sẽ được triển khai rộng rãi hơn (xem hình 12.2). Nhìn chung việc sử dụng các chứng nhận điện tử có chiều hướng tăng lên (cho thương mại điện tử hay e-mail bảo mật) và cần thêm một cơ chế trung tâm cho việc tạo và quản lý các máy chủ chứng nhận.

Khi dự định tạo một VPN, lúc chọn phần mềm chúng ta phải chọn sản phẩm hỗ trợ tốt những yêu cầu trên để đảm bảo mạng hoạt động hiệu suất, trôi chảy.

12.3 Tổng quan về các sản phẩm

Chúng ta có thể tham khảo một số sản phẩm phần mềm thông dụng cho VPN như bảng 12.1 bên dưới, lưu ý rằng giá cả của những sản phẩm này đã thay đổi do chúng được cập nhật vào năm 1998.

Bảng 12.1: Các phần mềm thông dụng cho VPN

	1	2	3	4	5
Sản phẩm	Alta Vista Tunnel 98 (Compaq)	Border manager (Novell)	Conclave (Internet Dynamics)	PrivateWire (Cylink)	RRAS/NT server (Microsoft)
Giá	$9951	$24954	$2495 (25 người dùng, không CA) $3995 (25 người dùng, CA)	$19004	Miễn phí !
Phần mềm máy chủ	Win NT, Digital unix	Solaris, SunOS, Netware,Win 95, NT	Win NT, Netware Unix	Win NT, Solaris	Win NT
Phần mềm truy cập từ xa	Win95, NT	Win95, NT	Win, Unix, MAC	Win 3.x, Win 95, NT	Win95, NT

	1	2	3	4	5
Giao thức định đường hầm	Độc quyền	Độc quyền	IPSec, PPTP	Độc quyền	PPTP
Giao thức hỗ trợ	IP	IP, IPX	IP	IP	IP, IPX, NetBEUI
Kiểu mã hoá	128 bit RC4	128 bit RC2	DES, Triple DES RC2,RC4	DES, Triple DES, RC4	RC4
Nhận dạng người dùng	SecurID, đoạn LAN	RADIUS	SecurID	CHAP, card riêng	Thẻ bài hoặc MSCHAP, PAP
Điều khiển truy cập	Không	Nguồn, đích, giao thức	Mức tài liệu, nguồn, đích		Lọc PPTP
Tích hợp quản trị người dùng	Miền người dùng NT	NDS	Windows ID, X.509	Độc quyền, thư mục	Miền người dùng NT
Quản lý khoá	RSA	SKIP	SKIP	Diff-Hellman	Diff-Hellman
Các nút được hỗ trợ	Không giới hạn				
Các đường hầm được hỗ trợ	2000 trên máy chủ Unix)				256
Tường lửa tích hợp	Không	Lọc gói, proxy ứng dụng	Lọc gói, proxy ứng dụng	Có	Không (cùng với NT Server)
Quản trị từ xa	Có	Có	Có	Có	Có
Các chứng nhận	Có		X.509	Có	Không
Client truy cập từ xa	Có	Không	Có	Có	Có
Nén	Có	Không	Không		Có

Một số sản phẩm đã trình bày trong bảng thực ra là tập hợp của nhiều sản phẩm khác. Nếu chúng ta không cần tất cả các dịch vụ đã liệt kê như trong bảng cho một sản phẩm cụ thể, ta nên kiểm tra xem nhà cung cấp có thực hiện những giải pháp không trọn gói hay không. Ví dụ như hãng Novell qüyết định cung cấp một số mô đun trong sản phẩm Borderguard của họ như những sản phẩm riêng lẻ.

Vấn đề kế tiếp mà chúng ta phải đảm bảo đó là tính cân bằng giữa các yêu cầu cho mạng với hiệu suất của một sản phẩm, đặc biệt khi ta đang dự tính cài đặt nhiều dịch vụ trên cùng một máy tính đơn, ta phải đảm bảo tính bảo mật cho máy tính này bằng cách thực hiện những biện pháp bảo mật để chống lại sự phá hoại của kẻ tấn công cũng như đảm bảo cho hoạt động bình thường phần cứng (ví dụ như thực hiện các biện pháp như sửa chữa, bảo quản định kỳ...).

Như ta đã từng nhận xét trong chương trước, thì việc sử dụng phần cứng VPN thay cho việc dùng phần mềm sẽ đạt được hiệu suất cao hơn bởi vì việc mã hoá bằng phần cứng sẽ có tốc độ nhanh nhiều hơn mã hoá bằng phần mềm. Tuy nhiên, hiện nay người ta vẫn sử dụng phần mềm, đó là do các lý do sau:

- Lý do thứ nhất: đây là lý do liên quan đến giá cả, dĩ nhiên việc dùng phần mềm thay vì dùng phần cứng sẽ có giá chi phí thấp hơn nhiều do một số phần mềm có giá tương đối rẻ, thậm chí một số phần mềm như RRAS của Microsoft còn cung cấp miễn phí khi ta mua hệ điều hành Windows NT.
- Lý do thứ hai: đây là lý do liên quan đến vấn đề sử dụng, chúng ta hầu như ai cũng quen thuộc với một hệ điều hành hay hệ điều hành mạng nào đó, mà các sản phẩm phần mềm VPN sẽ được cài trên đó. cho nên việc quản lý VPN sẽ gặp nhiều thuận tiện, lý thú hơn. Ngược lại, việc cài đặt một hệ điều hành mới sẽ gây cho chúng ta nhiều điều phiền phức do ta chưa quen với hệ điều hành này. Lấy ví dụ như khi đang sử dụng Unix, ít người lại muốn mua Win NT về cài, vừa tốn tiền vừa phải bỏ thời gian nghiên cứu hệ điều hành này.
- Lý do cuối cùng là các dịch vụ và hiệu suất mà những sản phẩm này cung cấp có thể là tất cả những thứ chúng ta cần đến. Nếu như ta đang xây dựng một VPN có quy mô nhỏ hay đang vận hành trên một lưu lượng thấp, ta có thể không cần đến mức hiệu suất tối ưu mà phần cứng VPN cung cấp, dĩ nhiên là cả vấn đề giá cả nữa: mạng nhỏ thì chúng ta không muốn đầu tư chi phí lớn cho các thiết bị phần cứng mà chỉ cần dùng những sản phẩm phần mềm là đủ yêu cầu hiện tại.

TỔNG KẾT

Hiện đang có nhiều sản phẩm dùng cho việc tạo nên VPN sử dụng các giao thức định đường hầm độc quyền và những sản phẩm không chuẩn dùng cho việc chuyển giao khoá đã làm hạn chế khả năng liên điều khiển. Nhưng kể từ năm 1998, nhiều sản phẩm đã trở nên tương thích với IPSec làm tăng thêm tính liên điều khiển giữa chúng.

Nếu ta không quan tâm đến việc liên điều khiển thì ta có thể sử dụng một số sản phẩm có chất lượng tốt hiện đang phổ biến ngoài thị trường. Ví dụ, phần mềm RRAS chạy trên nền Windows NT của hãng Microsoft thực sự là một máy chủ đường hầm (dùng giao thức PPTP) có tính năng tốt và đặc biệt là phần mềm này được cung cấp miễn phí khi chúng ta mua hệ điều hành Windows NT. Và sản phẩm Boderguard của hãng Novell rất thích hợp khi mạng của chúng ta đang hoạt động với giao thức IPX cũng như giao thức IP.

PHẦN III

QUẢN LÝ VPN

Để đảm bảo sự hoạt động liên tục của mạng, đặc biệt là những mạng lớn, người quản trị mạng phải nắm được đầy đủ và thường xuyên các thông tin về cấu hình, sự cố và tất cả số liệu liên quan đến việc sử dụng mạng.

Việc quản lý VPN gồm có ba phần: bảo mật, cấp phát địa chỉ IP và chất lượng mạng. Quản lý bảo mật không chỉ bao hàm việc xác thực những người dùng từ những vị trí khác nhau và điều khiển quyền truy cập mà còn quản lý các khoá mã liên kết với các thiết bị VPN. Các VPN thường liên kết lại với nhau trước khi tách riêng ra các mạng, điều này đòi hỏi mở rộng địa chỉ IP và quản lý tên qua toàn bộ tổ chức và có thể dẫn tới việc tranh chấp một con số.

Bạn nên liên kết việc quản lý địa chỉ và bảo mật của VPN để xác lập các chính sách và các dịch vụ thống nhất. Nhưng bạn có thể triển khai các công nghệ mới để cung cấp việc quản lý chất lượng trên các liên kết WAN thường sử dụng cho các VPN. Bạn sẽ không chỉ phân xử các dịch vụ mạng phân biệt tùy theo nhu cầu kinh doanh mà còn hoàn thiện các chính sách để mạng cung cấp chất lượng khác nhau cho những lớp khác nhau của lưu lượng. Cuối cùng, bạn tích hợp các yêu cầu chất lượng với khả năng mà ISP có thể cung cấp.

CHƯƠNG 13

QUẢN LÝ BẢO MẬT

Trong chương này chúng ta thảo luận các vấn đề về bảo mật các máy tính, các mạng và dữ liệu được lưu trữ trên các thiết bị truyền qua chúng. Trước tiên là một số vấn đề tổng quát về chính sách bảo mật thống nhất, những vấn đề liên quan đến bảo mật xung quanh việc quản lý VPN. Sau đó, chúng ta sẽ tập trung trên việc chọn lọc một số giải thuật mã hoá và các chiều dài khoá, phân phối các khoá và liên kết thông tin trong tập liên kết bảo mật IPSec, cũng như xác thực người dùng và điều khiển quyền truy cập. Vì tầm quan trọng của việc xác thực những người dùng và thiết bị với các chứng nhận điện tử nên chúng ta sẽ thảo luận chi tiết việc quản lý nội bộ các chứng nhận.

IPSec đưa ra vùng chọn lựa lớn nhất để bảo mật dữ liệu với bất kỳ giao thức nào và bao hàm kiến trúc phức tạp nhất để điều hành và hỗ trợ các chọn lựa này. Vì có nhiều lựa chọn và phức tạp, nên việc quản lý bảo mật cho VPN sẽ tập trung trên IPSec, có bao hàm PPTP và L2TP ở những vị trí thích hợp.

13.1 Những chính sách bảo mật thống nhất

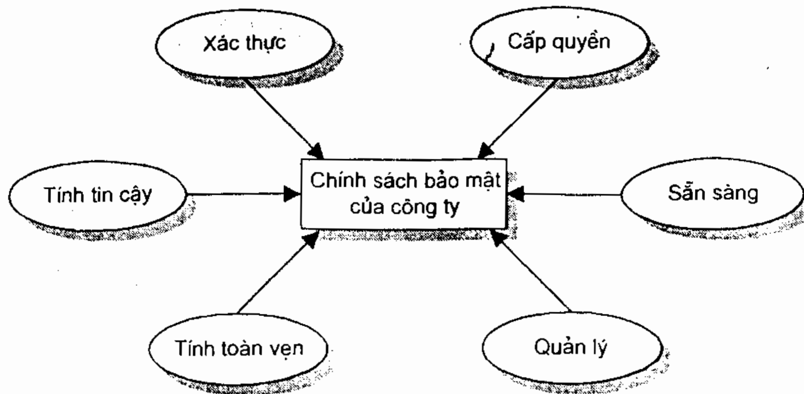
Để thực hiện việc bảo mật thống nhất có nhiều phương pháp hơn những gì sẽ được trình bày. Một khung làm việc bảo mật riêng cho một tổ chức bao hàm 7 yếu tố khác nhau: xác thực, tính bảo mật, tính nguyên vẹn, cấp quyền, tính sẵn sàng, quản lý và độ tin cậy (phát hiện hỏng hóc) (xem hình 13.1).

Nối mạng bảo mật chỉ là một phần của bảo mật thống nhất, nó là một phần quan trọng và sẽ có vị trí trong các chính sách bảo mật thống nhất.

Một cơ chế bảo mật tổng quát nên thực hiện như sau:

- Xem xét những gì bạn đang bảo mật.
- Xem xét những gì bạn cần bảo mật từ đâu.

- Xác định các nguy cơ có thể.
- Tiến hành đánh giá những việc sẽ bảo mật trong phương pháp xác thực giá.
- Xem xét việc xử lý một cách liên tục.
- Hoàn thiện mọi thời gian thực.



Hình 13.1: Các thành phần của hệ thống bảo mật

Chính sách bảo mật truyền thống nhận biết tất cả các tài sản trong cơ sở hạ tầng thông tin thống nhất đang được bảo mật, cơ sở dữ liệu tập trung và phần cứng máy tính. Chính sách này sẽ bao hàm mọi mặt từ việc truy cập vật lý tới việc sở hữu, việc truy cập chung tới các hệ thống thông tin và việc truy cập đặc biệt tới các dịch vụ trên các hệ thống này.

Nhưng, khi các hệ thống thông tin đã trở nên phân tán hơn, các chính sách bảo mật thống nhất có bao hàm các nguyên tắc quản lý trên phạm vi các LAN. Các phương tiện bổ sung các chính sách dựa trên việc truy cập tới các tài nguyên trong những phạm vi khác. Cụ thể, như có thể truy cập các máy chủ dành cho việc nghiên cứu và phát triển (R&D) không hoặc ai có thể đọc thư của người quản lý?

Khi định nghĩa các chính sách bảo mật cho mạng thì cần nhận biết mọi điểm truy cập tới hệ thống thông tin và định nghĩa các nguyên tắc của chính sách để bảo mật các điểm vào/ra. Không thể bỏ qua các modem được dùng trong cơ quan, nó có thể là các điểm truy cập hấp dẫn đối với những người tấn công khi những người dùng bên trong quay số sử dụng các dịch vụ trực tuyến.

Một vài vấn đề khi lập một chính sách bảo mật:

- Việc tổ chức kế hoạch sử dụng các dịch vụ Internet?
- Cần bổ sung những gì (mã hoá...) để có thể được hỗ trợ?
- Các dịch vụ sẽ được sử dụng ở đâu? Chúng có được sử dụng trên LAN hoặc truy cập từ xa không?

- Điều gì sẽ xảy ra khi liên kết việc cung cấp các dịch vụ và truy cập.
- Định giá cái gì trong giới hạn của điều khiển và tác động trên mạng không tin cậy được cung cấp bảo mật?
- Phí tổn để thực hiện được việc bảo mật?.

Toàn bộ kế hoạch bảo mật là khả năng giám sát và đáp ứng đến các biến cố phức tạp xảy ra. Như một phần chính của chính sách bảo mật, nên định nghĩa một thủ tục đáp ứng sự cố.

Một trong những chính sách bảo mật mới lưu hành được phát hiện ở VPN là quản lý khoá. Trong phần trước, nếu sử dụng một kênh thuê riêng VPN, mã hoá lớp liên kết có thể được sử dụng mà không yêu cầu thay đổi các khoá mật mã. Nhưng, tính chất động và tính mềm dẻo của các VPN trên cơ sở Internet yêu cầu phân phối các khoá rộng hơn và tái định khoá lại thường xuyên hơn nên yêu cầu các hệ thống phức tạp hơn để quản lý khoá. Điều này đúng khi người dùng từ xa gặp khó khăn.

Về dung lượng của lưu lượng qua giữa các host, cần bảo mật dung lượng để chống lại xâm phạm, ví dụ như các virus máy tính, phần này cũng quan trọng trong chính sách bảo mật. Các virut máy tính được phân phát qua e-mail, chương trình, tài liệu bị nhiễm, do vậy phải ngăn ngừa lây lan do truyền bá, để bảo mật đầy đủ nên có phần mềm chống virut.

Sau đây là một vài chi tiết của việc quản lý bảo mật VPN.

13.2 Chọn lọc các phương thức mã hoá

Khi bạn tạo lập một VPN, có hai bắt buộc chính trên việc bảo mật dữ liệu của bạn theo mức độ yêu cầu (bạn sẽ sử dụng sau khi chọn các giao thức VPN). Thứ nhất: ngay khi một số giao thức như IPSec hỗ trợ các trạng thái khác nhau của các giao thức mã hoá trong các kỹ thuật, không phải tất cả các sản phẩm đều bao gồm mọi giải thuật mã hoá. Thứ hai: là các quốc gia đặc biệt hạn chế xuất các chiều dài khoá. Cụ thể, ở Mỹ bạn thường xuyên bị hạn chế sử dụng các chiều dài khoá 40 bit hoặc 56 bit với DES để mã hoá, mặc dù vậy bạn cũng có thể sử dụng khoá có chiều dài 128 bit.

Sau đó bạn tập hợp, phân tích dữ liệu thống nhất và chọn lọc các sản phẩm cho VPN, bạn có thể chọn các chiều dài khoá và các giải thuật thích hợp.

13.2.1 Các giao thức và giải thuật cho VPN

Các giao thức của VPN như IPSec, PPTP và L2TP trình bày rõ các danh mục riêng của các giải thuật được cho phép để mã hoá dữ liệu.

Mặc dù PPTP có thể sử dụng PPP và các chọn lựa mã hoá giao dịch được (bao gồm DES và Triple DES) để mã hoá dữ liệu, Microsoft có hợp nhất một phương thức mã hoá gọi là mã hoá điểm-điểm MPPE (Microsoft Point-to-Point Encryption) để sử dụng với các đường hầm PPTP. MPPE sử dụng giải thuật RC4 với các khoá 40 bit hoặc 128 bit, tuỳ thuộc trên giới hạn xuất. Tương tự, L2TP có thể sử dụng PPP để mã hoá dữ liệu, nhưng phương thức nêu ra trước sử dụng IPSec cho tác vụ này.

Trong IPSec, giải thuật mã hoá mặc định để sử dụng trong ESP là DES với một định hướng ban đầu rõ ràng. IPSec cho phép các giải thuật luân phiên sử dụng. Nó bao gồm Triple DES, CAST-128, RC5, IDA, Blowfish và ARCFour (một sự thực hiện chung của CR4).

Các nhà cung cấp chọn lựa các giải thuật hỗ trợ khác DES, do vậy có thể tìm thấy các sản phẩm của nhà cung cấp không hỗ trợ việc lựa chọn giải thuật để có kế hoạch sử dụng. DES và Triple DES có thể là giải thuật chung nhất hỗ trợ từ xa. Do vậy cần phải xác định lợi ích để lựa chọn các giải thuật mã hoá: có thể người xâm phạm không chỉ phá mật mã mà còn xác định mật mã họ muốn phá.

Trở lại kiểu Oakley sử dụng trong IPSec, kiểu chính để xem xét các phương thức mã hoá, các hư hỏng, phương thức xác thực và nhóm Diffie-Hellman giữa các điểm cuối VPN. Nhóm Diffie-Hellman xác định khả năng của phương tiện chỉ định khoá; có 4 nhóm Diffie-Hellman. Nhóm Diffie-Hellman thứ nhất đủ mạnh cho DES, nhóm 2 và nhóm 3 nên sử dụng cho Triple DES. Vì kiểu chính phải yêu cầu 6 gói, nên nếu bạn đang sử dụng cho các kết nối vệ tinh có thời gian chờ cao, nó sẽ tốt hơn cho DES nếu sử dụng nhóm Diffie-Hellman mạnh hơn.

Kiểu nhanh hơn của Oakley cũng xem xét các giải thuật và thời gian sống cho IPSec. Xác định thời gian sống như thế nào thường dựa trên thời gian hoặc dữ liệu, kiểu nhanh khác xem xét yêu cầu. Thời gian sống của kiểu chính điều khiển Oakley SA và thời gian sống của kiểu nhanh điều khiển IPSec SA. Ví dụ, thời gian sống của kiểu nhanh có thể đặt 15 phút hoặc 10 MB và thời gian sống của kiểu chính đặt là một giờ hoặc 40 MB, khi DES bắt đầu sử dụng cho IPSec. Thời gian sống có thể tăng cho Triple DES vì nó bảo mật hơn DES hoặc giảm đối với ARCFour vì nó kém bảo mật hơn DES. Ý tưởng để cân bằng độ mạnh của các dịch vụ IPSec và độ mạnh của các giải thuật mã hoá căn bản tương phản với giá của tiêu đề gói ISAKMP/Oakley; nhiều thay đổi trong các khoá có thể tác động đến hiệu quả mạng.

13.2.2 Các chiều dài khoá

Cần phải xác định độ nhạy của dữ liệu để bạn có thể tính toán nó nhạy bao lâu và nó sẽ được bảo mật trong bao lâu. Khi tính được, bạn có thể chọn một giải

thuật mã hoá và chiều dài khoá để thời gian phá lâu hơn chiều dài thời gian nhạy của dữ liệu.

Trước tiên, xem bảng 13.1, là những thông tin tóm lược từ cuốn sách của Brude Schneier, *Thực hành mã hoá* (Applied Cryptography). Bảng này cũng là công việc hữu ích minh họa nhiều chiều dài khoá được sử dụng hiện nay có thể bị phá với một chỉ tiêu phí tổn không lớn. Bảng này cũng giúp làm nổi bật một điểm là: biết người xâm phạm. Nếu là những chuyên gia họ sẽ cố gắng mã hoá và giải mã dữ liệu, khi đó chiều dài khoá dài và việc khoá lại thường xuyên là cần thiết.

Bảng 13.1 Đối chiếu với thời gian và phí tổn cần thiết để phá các khoá.

Giá (USD)	Chiều dài khoá theo bit				
	40	56	64	80	128
100 ngàn	2 giây	35 giờ	1 năm	70.000 năm	10^{19} năm
1 triệu	2 giây	3,5 giờ.	37 ngày	7.000 năm	10^{18} năm
100 triệu	2 ms	2 ms	9 giờ	70 năm	10^{16} năm
1 tỉ	2 ms	13 giây	1 giờ	7 năm	10^{15} năm
100 tỉ	2 ms	1 giây	32 giây	24 ngày	10^{13} năm

Với khả năng bẻ khoá không chuyên thì chỉ có thể phỏng đoán. Có nhiều phương thức khác nhau cho việc phá các khoá, tuỳ thuộc vào mật mã sử dụng dùng để phân tích mã, nhưng đánh giá cho xâm phạm không chuyên là dẫn chứng chung khi đo độ mạnh của phương thức mã hoá.

Cần ghi nhớ rằng đây không phải là trạng thái tĩnh. Nguồn máy tính luôn thay đổi và giá đang giảm do vậy trong tương lai để phá khoá lớn sẽ dễ và rẻ hơn. Sản phẩm Off-the-shelf processing (giá khoảng 500 nghìn USD) có thể phá mã DES 56 bit trong 19 ngày; người tấn công chọn đầu tư trong các vi mạch khách hàng có thể phá mã trong ít giờ. Một sinh viên ở UC Berkeley sử dụng mạng với 250 trạm làm việc để phá giải thuật RC5 trong 3 giờ 30 phút.

13.3 Quản lý khoá cho các cổng nối

Một số các khoá thường được yêu cầu để bảo đảm liên lạc bảo mật giữa các cổng nối. Thứ nhất: là có một cặp khoá để nhận dạng 2 cổng nối khác nhau, các khoá này phải được nối kết cứng, thay đổi nhân công hoặc truyền qua các chứng nhận điện tử. Thứ hai: là các khoá phiên yêu cầu xác thực và mã hoá các gói được truyền giữa các cổng nối, cụ thể, sử dụng các tiêu đề AH và ESP của IPSec. Các khoá khác nhau được yêu cầu cho mỗi tiêu đề IPSec và được xem xét qua

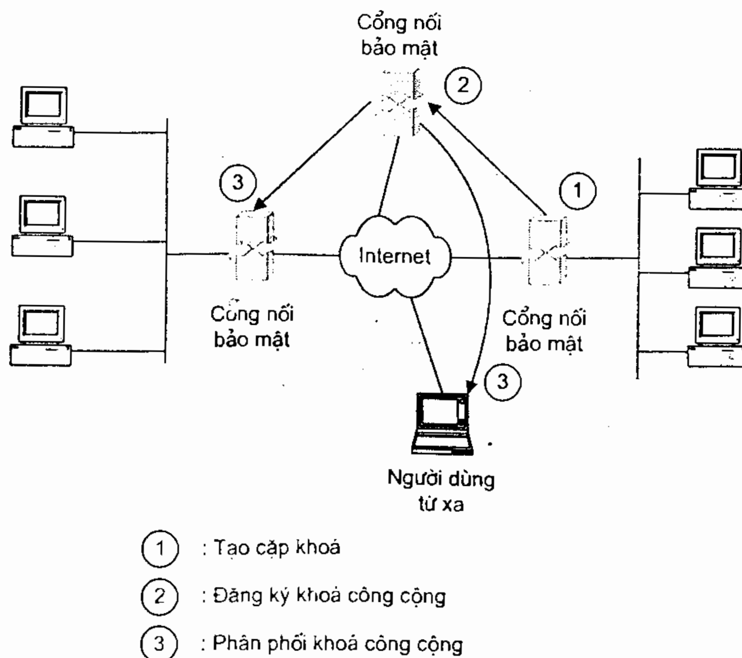
các liên kết bảo mật. Cụ thể nếu cả AH và ESP được sử dụng để xử lý các gói, khi đó hai SA được xem xét giữa các cổng nối hoặc các host.

13.3.1 Nhận dạng các cổng nối

Trước tiên một đường hầm bảo mật có thể được thiết lập giữa hai cổng nối bảo mật hoặc giữa một host từ xa và một cổng nối, các thiết bị này đã được xác thực bởi một thiết bị khác và được chấp thuận trên một khoá. Đầu tiên, hãy xem thay đổi giữa hai cổng nối. Xác thực này không đồng thời với xác thực các gói sử dụng tiêu đề AH, ở đây các thiết bị tự xác thực.

Các cổng nối sử dụng các cặp khoá chung có thể được xác thực nhân công. Trong trường hợp này, cặp khoá thường kết nối cứng trong thiết bị trước khi nó được sắp xếp. Sau đó người quản lý mạng ghi các thiết bị mới với các cổng nối bảo mật khác trên VPN, đưa ra các cổng nối này khoá chung do đó có thể thay đổi các khoá phiên.

Nếu một cổng nối bảo mật không được xếp với các khoá nối kết cứng, cổng nối sẽ thiết lập để đưa ra ngẫu nhiên cặp khoá riêng của nó. Khi đó một chứng nhận điện tử sẽ được chỉ định với khoá riêng và gửi đến quyền đăng nhập chứng nhận thích hợp, một máy chủ chứng nhận nội bộ hoặc CA cấp 3 như VerSign. Khi chứng nhận được chấp nhận, chứng nhận này sẵn sàng từ CA để sử dụng bởi các cổng nối bảo mật khác và các client từ xa tới xác thực vị trí trước khi dữ liệu được thay đổi (xem hình 13.2).



Hình 13.2: Chuyển giao khoá giữa các cổng nối

Mặc dù các chứng nhận này không cần chuẩn hoá (cụ thể là sử dụng chuẩn X.509) nếu các sản phẩm của nhà cung cấp chỉ được sử dụng cho VPN, khả năng liên vận hành giữa các sản phẩm có thể thực hiện được khi các chứng nhận X.509 được dùng. Nhiều nhà cung cấp đã đồng nhất phương pháp này để dễ sử dụng tác quyền chứng nhận bên ngoài cho việc lưu trữ các chứng nhận cần thiết. Điều này là cần thiết nếu bạn đang mở rộng VPN để bao hàm các đối tác trong một Extranet.

Các cổng nối khác và các host từ xa thường thu được chứng nhận thích hợp từ CA tới xác thực cổng nối đích bằng việc sử dụng cơ chế như LDAP hoặc HTTP để hạn chế thông tin chứng nhận qua cấu trúc khoá công cộng PKI (Public Key Infrastructure). PKI đang tồn tại cũng yêu cầu kiểm tra danh sách thu hồi chứng nhận CRL (Certification Revocation Lists) để đảm bảo hiệu lực của chứng nhận đang tồn tại. Vì hệ thống CA cho các trạng thái khác nhau của các chứng nhận trở nên không hợp lý và CLR có thể trở nên phức tạp để điều khiển được, một cơ chế khác đối với trạng thái khác nhau của các chứng nhận được phát triển. Chi tiết, nhóm làm việc IETF PKIX đang định nghĩa một khả năng liên vận hành PKI và giao thức trạng thái chứng nhận trực tuyến OCSP (Online Certificate Status Protocol). Các tiêu chuẩn OCSP cung cấp phương thức có hiệu quả để điều khiển phân xử và hủy bỏ các chứng nhận.

Các hệ thống này là cơ sở dựa trên việc chỉ định cặp khoá chung tới mỗi cổng nối và một khoá chung được xuất trong một thư mục đó là khả năng truy cập tới tất cả các vị trí của VPN. Khi bắt đầu một phiên mã hoá, khoá phiên bị tranh chấp bởi sự kết hợp giữa khoá riêng của cổng nối bảo mật với khoá chung của người dùng.

13.3.2 Điều khiển các khoá phiên

Nếu thay đổi khoá (giống như trong IPSec và L2TP) được yêu cầu giữa các vị trí, phương thức cơ bản nhất là thay đổi nhân công các khoá. Một khoá phiên ban đầu được sinh ra ngẫu nhiên bởi một cổng nối bảo mật và sau đó người quản lý mạng phân phối khoá để quản lý thiết bị thứ cấp, cụ thể là máy điện thoại, ghi thư hoặc kết hợp thư tín. Quản lý thứ cấp đặt khoá đến cổng nối bảo mật thứ cấp và một phiên bảo mật giữa hai cổng nối được lập. Các khoá mới được sinh ra khi có yêu cầu và được phân phối trong cùng một phương cách như trước.

Bảo mật trên cơ sở phần cứng

Các sản phẩm mã hoá trên cơ sở phần cứng không bị ảnh hưởng bởi xâm phạm vật lý nên giảm cơ hội các khoá thiết bị được thỏa thuận và do đó cần thay đổi các khoá mới giữa các cổng nối. Các khoá có hoặc không có nối kết cứng

hoặc nhập vào từ một trạm quản lý, hầu hết bộ mã hoá phần cứng được niêm phong bền vững trái với thông tin vật lý và thường bị xóa bất kỳ, khoá được lưu trữ khi bất thường.

Phương pháp này chậm hơn và không bảo mật tuyệt đối; các đường điện thoại có thể được xác định rõ và thư có thể bị ngăn lại. Quản lý khoá động, cụ thể là sử dụng IKE sẽ dễ và tốt hơn để thường xuyên thay đổi khoá và số lượng vị trí lớn. Các khoá phiên được đưa ra ngẫu nhiên từ cổng nối bảo mật đầu tiên hoặc máy chủ quản lý khoá và phân phối trên mạng. Khoá phiên tự dành quyền sử dụng khoá chung của người nhận trước khi truyền trên mạng.

Nếu các khoá phiên được thỏa thuận bạn cần có một phương pháp để hủy bỏ một cặp khoá và chỉ định bằng một cặp mới. Các thủ tục để hủy bỏ khoá khác nhau giữa các sản phẩm. Các cổng nối bảo mật đáp ứng để hủy bỏ khoá cũng khác nhau các sản phẩm. Phương thức bảo mật nhất là dừng phiên và nhập vào lỗi, cố gắng nhanh chóng hủy bỏ khoá được phát hiện. Một vài thủ tục chờ một phiên được hoàn thành trước khi từ chối truy cập khoá này.

Nếu trong vùng nơi mà VPN hạn chế các khoá chiều dài ngắn (do giới hạn xuất) khi đó phải cố gắng hoàn thiện các phiên VPN bảo mật bằng việc thường xuyên khoá lại. Nếu các khoá được sử dụng với chiều dài ngắn hơn, khi đó bất kỳ xâm phạm nào cũng sẽ có ít thời gian để thu được thông tin cần thiết cho việc phá một khoá, tổng số dữ liệu đó có thể thu được với một khoá sẽ giảm.

13.4 Quản lý khoá cho các người dùng

Các khoá được đưa ra và được phân phối cho VPN kết nối LAN-LAN có thể xử lý một cách tương đối đơn giản để quản lý khi số lượng vị trí không quá lớn. Thậm chí, nếu số vị trí nhỏ hơn 100, một hệ thống động sử dụng tác quyền chứng nhận bên ngoài hoặc máy chủ chứng nhận nội bộ nên không làm phức tạp phân phối rộng lớn của việc quản lý tiêu đề. Quản lý các khoá đối với người dùng từ xa, với số lượng hàng ngàn, cần phải sắp xếp và tự động khi có thể. Một hệ thống tự động được yêu cầu nếu bạn có kế hoạch sử dụng bảo mật trong IPSec. Phân phối các khoá và liên kết thông tin có thể vô hiệu và hao tốn thời gian.

Một cặp các thiết bị IPSec để thiết lập liên kết bảo mật với thiết bị khác trong thứ tự truyền thông. Nếu bạn đang có kế hoạch để hỗ trợ số lượng lớn người dùng truy cập từ xa với một cổng nối bảo mật, khi đó bạn cần phải đưa ra liên kết bảo mật client một cách tập trung. Trong thực tế, hầu hết các trung tâm đưa ra tất cả các thông số IPSec SA cần thiết và cung cấp một cơ chế xuất chúng bên trong client. Ví dụ, một vị trí trung tâm có thể đưa ra dữ liệu SA trong định dạng S/WAN và gửi thông tin thích hợp tới các client khác nhau.

Kiến trúc IPSec giúp các host chỉ định chỉ số tham số bảo mật SPI (Security Parameter Index) để các tiêu đề IPSec trở về, với yêu cầu SPI đó là duy nhất. Nếu bạn thiết lập một vị trí trung tâm để đưa ra chỉ tiêu khoá và chỉ định ISP tới sử dụng, khi đó phần mềm client có thể sử dụng SPI này cho việc truyền thông không cần đưa ra bất kỳ SPI riêng lẻ.

Người dùng VPN từ xa được xác thực bởi các cổng nối bảo mật giống như khi cổng nối tự nhận dạng tới mỗi cổng nối bảo mật khác và được xác thực. Số lựa chọn cho người dùng đăng nhập là rất lớn. Vì việc sử dụng chứng nhận điện tử để nhận dạng người dùng trở nên phổ thông hơn và hỗ trợ bởi các sản phẩm VPN nên sẽ được thảo luận chi tiết về vấn đề quản lý chứng nhận cho người dùng trong phần "13.6 Quản lý CA nội bộ" trang 192.

Việc bảo mật các client chống lấy cắp

Bởi vì các máy xách tay dễ bị lấy cắp, họ sẽ điều tra bảo mật đặc biệt tới VPN của bạn bởi vì các khoá lưu trữ trên các máy xách tay bị mất có thể được sử dụng để truy cập các tài nguyên thống nhất qua VPN.

Có 3 công nghệ chính để bảo mật các khoá:

- Lưu trữ các khoá trên một thiết bị di dời được như đĩa hoặc card thông minh và mang nó riêng lẻ từ các client.
- Mã hoá khoá với một mật khẩu hoặc cụm từ và yêu cầu client xác nhận mật khẩu trước khi IPSec được sử dụng (các card thông minh có thể làm rất tốt việc này).
- Mã hoá các khoá với một mật khẩu và một cụm từ và ngăn cản các tiến trình IPSec nếu sử dụng sai mật khẩu.

Có 3 lựa chọn này là an toàn nhất. Nhưng, điều này cũng gây phiền phức với người sử dụng hợp pháp khi tình cờ vào sai mật khẩu bởi vì không thể biết lý do cho một lỗi truyền thông.

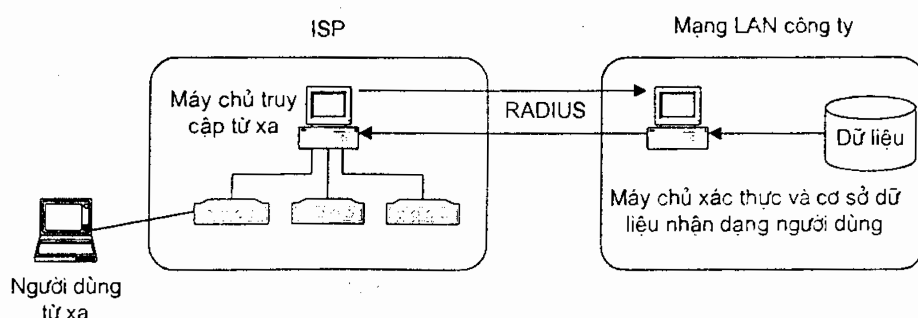
13.5 Các dịch vụ xác thực

Có nhiều cách khác nhau để xác thực các người dùng vào mạng: các mật khẩu đơn giản, các mật khẩu một lần, các hệ thống lệnh/đáp ứng sử dụng RADIUS hoặc TACACS+ hoặc các hệ thống 2 nhân tố sử dụng các thẻ bài, cũng như các chứng nhận điện tử. Cụ thể, nếu bạn đã hỗ trợ truy cập từ xa qua modem và máy chủ truy cập từ xa, khi đó bạn đã có một vị trí trong hệ thống xác thực và bạn cần liên kết nó tới cổng nối bảo mật của bạn để điều khiển xác thực và quyền truy cập của các người dùng VPN.

Nếu sử dụng PPTP, L2F hoặc L2TP để tạo các đường hầm, dùng ISP của bạn như một điểm cuối đường hầm. Ở trường hợp này, ISP nên chạy máy chủ xác thực riêng của nó chính là ủy quyền tới máy chủ xác thực của bạn (xem hình 13.3). Điều này cho phép bạn duy trì điều khiển việc thiết lập các thông số xác thực và các quyền truy cập nhưng cản trở ISP dùng thông tin đó để cung cấp việc truy cập tới những người dùng truy cập từ xa của bạn.

Bạn có thể cài đặt một hệ thống xác thực VPN, thì bạn có thể chọn bất kỳ phương pháp nào. Các hệ thống tốt là RADIUS, xác thực trên cơ sở thẻ bài và các chứng nhận điện tử.

RADIUS có 3 thuận lợi. Nó được chuẩn hoá bởi IETF và nhiều nhà cung cấp đưa ra các sản phẩm liên vận hành đó. RADIUS cũng sử dụng tính đa số của ISP cho việc xác thực các khách hàng. Cuối cùng, RADIUS có thể thi hành như một cơ sở dữ liệu xác thực trung tâm, thể hiện trên định nghĩa các quyền cho các người dùng từ nhiều loại hệ thống mạng khác nhau đang hoạt động như các miền người dùng của NT và cây NDS, làm nó thích hợp đối với thống nhất.



Hình 13.3: Các máy chủ xác thực

Cả RADIUS và TACACS+ cho phép bạn định nghĩa xác thực qua các trạng thái phiên khác nhau như thế nào, như các kiểu giao thức, các địa chỉ và các thông số khác. Đặc tính quan trọng về khả năng của cả hai hệ thống là định nghĩa các cơ chế điều khiển truy cập trên nền máy chủ. Các cơ chế này bao gồm việc hạn chế kiểu TOD, chỉ tiêu thông dụng, điều khiển nhập vào đồng thời (mỗi người dùng chỉ có thể sử dụng một phiên tại một thời điểm) và nhập vào ngưỡng xâm phạm (tài khoản bị khoá sau 10 số liên tiếp nhập sai). RADIUS cũng có thể được sử dụng cho các mục đích tài khoản, mặc dù chỉ tiêu đem thi hành các yêu cầu không làm thay đổi thời gian trực tuyến của mỗi người dùng khác nhau và có thể trở nên một tác vụ tương đối quan trọng.

Một máy chủ RADIUS bao gồm 3 tệp chính: một cơ sở dữ liệu để các người dùng đăng nhập, một tệp của client truy cập các máy chủ chính nó được quyền yêu cầu các dịch vụ xác thực và một tệp các lựa chọn của khách hàng, gọi là các từ điển cho mỗi máy chủ truy cập từ xa và cổng nối bảo mật. Cụ thể, nếu bạn đang cấu hình RADIUS để sử dụng với ISP và PPTP, bạn sẽ thêm tên hoặc địa chỉ của máy chủ ủy quyền của ISP tới tệp client truy cập các máy chủ và định nghĩa một từ điển mới cho máy chủ này, mô tả bất kỳ xác thực đặc biệt và các đặc tính tác quyền cho các máy chủ (TACACS không bao hàm các từ điển trong kiến trúc của nó).

Xác thực trên cơ sở thẻ bài thường yêu cầu sử dụng tác động đặc biệt tới trạm làm việc hoặc các máy xách tay và một card thẻ bài để đưa ra các mật mã đặc biệt được kiểm tra bởi một máy chủ bảo mật trên mạng trước khi chỉ định truy cập tới người dùng. Trước khi người dùng được phép tự xác thực, các thiết bị thẻ bài yêu cầu một số nhận dạng cá nhân PIN. Hai kỹ thuật phổ thông hơn cho những người dùng khác nhau là một hệ thống lệnh/đáp ứng hoặc đồng bộ hoá thời gian, điều này tùy thuộc vào các đồng hồ đồng bộ hoá và khoá bí mật được thay đổi thường xuyên để người dùng vào khi đăng nhập. Mặc dù các thẻ bài là phương thức bảo mật cho xác thực, vì sử dụng phương thức 2 nhân tố nên bất tiện cho người dùng vì yêu cầu phần cứng bổ sung.

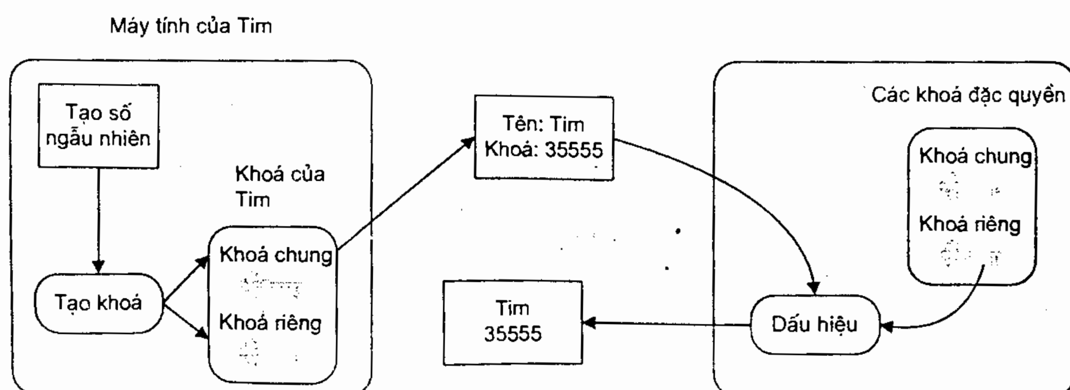
Nó cũng có thể sử dụng các chứng nhận điện tử để xác thực người dùng, mặc dù các hệ thống không phổ biến như các máy chủ RADIUS. Điều đó có thể thay đổi với thời gian. Các công việc của bạn đã có thể sử dụng các chứng nhận điện tử cá nhân với người duyệt Web hoặc các client e-mail. Nếu bạn đã gửi e-mail bảo mật để yêu cầu các chứng nhận điện tử và một cơ sở hạ tầng khoá chung, khi đó bạn có thể sử dụng trong cùng một hệ thống để cấp phát và lưu trữ các chứng nhận điện tử yêu cầu đối với xác thực trên VPN. Nếu không, bạn sẽ cài đặt một quyền đăng nhập chứng nhận thích hợp cho những người dùng của bạn, điều này có thể là một CA dự phòng và thu lại khoá, tự động cập nhật cặp khoá (và các chứng nhận) và quản lý nguồn gốc khoá.

Sử dụng quyền đăng nhập chứng nhận cấp 3 giúp ta quản lý chứng nhận dễ hơn, vì nó sẽ được thực hiện qua Internet và sẵn sàng truy cập tới bất kỳ các cộng tác của Extranet. Nhưng, nếu bạn đang hỗ trợ những người dùng bên trong, nên sử dụng đồng thời một CA nội bộ. Vì các cổng nối bảo mật sẽ thực hiện xác thực các người dùng của VPN, việc truy cập bên ngoài tới các chứng nhận điện tử là không cần thiết. Nhưng bạn vẫn cần bảo mật máy tính được sử dụng để cấp phát và lưu trữ các chứng nhận điện tử như các tệp dự phòng hoặc các thiết bị sao lưu.

Bất kỳ một vận hành nào bạn chọn, bạn sẽ cần một phương pháp phân phối tới mỗi người dùng các chứng nhận điện tử và các khoá riêng. CA bên ngoài thường điều khiển phân phối chứng nhận qua e-mail hoặc HTTP. Nếu bạn đang chạy máy chủ chứng nhận riêng, bạn có thể làm đồng thời, nhưng chính bạn phải chọn một phương tiện vật lý như một đĩa mềm hoặc card thông minh. Nhiều công ty thường dùng các card thông minh để phân phối và lưu trữ các chứng nhận điện tử vì chúng có khả năng mang đi và thực tế chúng cũng có thể hỗ trợ việc bảo mật với một PIN người dùng đặc biệt, điều đó làm card không sử dụng được nếu bị mất hoặc mất cắp. Có một lợi thế là các card này ngưng hoạt động khi nhập vào các lỗi liên tiếp.

13.6 Quản lý CA nội bộ

Các chứng nhận điện tử có một chu kỳ sống hữu hạn (xem hình 13.4); sau khi chúng được cấp phát một thời gian chúng sẽ ngưng (cụ thể là 6 tháng) hoặc có thể bị hủy bỏ nếu người chủ thay đổi công việc hoặc một khoá riêng được thỏa thuận. Các chứng nhận cũng có thể được tái lập và cần được dự phòng trong trường hợp các khoá cần được thu hồi sau một ngày. Nếu bạn muốn chạy quyền đăng nhập chứng nhận riêng trong nội bộ, quản lý hệ thống không chỉ đòi hỏi tạo các cặp khoá và cấp phát các chứng nhận mà còn quản lý các khoá và các chứng nhận này. Quản lý chứng nhận bao gồm việc duy trì nơi chứng nhận, từ chối chứng nhận khi cần và cấp phát bản kê khai hủy bỏ các chứng nhận CRL (Certification Revocation Lists). Quản lý khoá đòi hỏi khoá dự phòng và thu lại khoá, tự động cập nhật cặp khoá (và các xác thực) và quản lý nguồn gốc khoá.



Hình 13.4: Chu kỳ sống của một chứng nhận điện tử

OCSP: Một phương pháp động để kiểm tra các chứng nhận

Hiện nay không có phương tiện hữu dụng để hủy bỏ một chứng nhận nếu mật khẩu để mở chứng nhận của người sử dụng bị phá hoặc khi khoá riêng của người dùng được thỏa thuận. Giải pháp duy nhất các máy chủ chứng nhận đưa ra là danh sách CRL. Cơ bản nhất là xem chuẩn PKI và giao thức trạng thái chứng nhận trực tuyến OCSP (Online Certification Status Protocol) cho một giải pháp thực tế.

Phương pháp duy nhất để có thể sử dụng CRL là hợp hai danh sách (một danh sách trong bộ nhớ cục bộ và một danh sách trong CRL) và xóa các chứng nhận bằng tay. OCSP di chuyển liên tục từ kiểu danh sách tĩnh tới kiểu danh sách động hơn. OCSP định nghĩa các vấn đề về trạng thái LDAP và HTTP được thiết kế để cung cấp thời gian đáp ứng nhanh và lợi ích lớn. Trong đáp ứng tới một client, một máy chủ OCSP gửi thông báo trạng thái đơn giản - có hiệu lực, không có hiệu lực, hủy bỏ, không hủy bỏ hoặc ngừng lại. Sử dụng kiểu này, tải cân bằng giữa client và máy chủ và nó trở nên thi hành được việc kiểm tra chứng nhận thời gian thực trên mỗi giao tác cơ sở.

Khi bạn có kế hoạch triển khai máy chủ chứng nhận riêng, duy trì cơ sở hạ tầng cho các chứng nhận điện tử và quản lý chứng nhận vẫn được triển khai. Việc sử dụng CRL để giám sát hủy bỏ các chứng nhận là không đủ cho tình trạng động, có thể bạn sẽ đụng độ với người đang truy cập VPN từ xa. Nhưng, các giải pháp mới, như giao thức trạng thái chứng nhận trực tuyến OCSP (Online Certification Status Protocol), cũng đang được triển khai. Hơn nữa, máy chủ chứng nhận sẵn sàng cần hoàn thiện để hỗ trợ cho các tác vụ quản lý. Các hệ thống CA nội bộ của các công ty Certco Inc, Entrust Technologies Inc, GTE CyberTrust Inc, Microsoft Corp, Netscape Communications Corp, Security Dynamic Technologies Inc và Xcert Software Inc. Một số nhà cung cấp sản phẩm VPN xem CA như một bộ phận, mặc dù nhiều sản phẩm này là CA dựa trên nền phần mềm thiết lập trên một trạm làm việc. Radguard đưa ra chỉ định CA trên cơ sở phần cứng để sử dụng với CIPro.

Bất chấp mọi vấn đề, một máy chủ chứng nhận riêng có thể được thiết lập và được quản lý bên trong một tập đoàn để xác thực cả cổng nối và những người dùng trên mạng.

Tác vụ cơ bản của máy chủ chứng nhận là chấp nhận yêu cầu cho các chứng nhận mới, hàng đợi để xem lại bằng hệ thống quản lý và cấp phát các chứng nhận để client truy tìm (xem hình 13.5). Nhìn chung, các máy chủ chứng nhận chấp nhận các yêu cầu chứng nhận từ một trạm quản lý chứng nhận, khi bộ quản lý thực hiện cấp phát các chứng nhận từ chính họ hoặc qua HTTP hoặc e-mail.

Bất cứ khi nào các yêu cầu mới đối với các chứng nhận được nhận, chúng sẽ được tương thích trái với các chứng nhận giữ trong thư mục để ngẫu nhiên cản trở tình trạng cũ của các khoá chung có hiệu lực. Chứng nhận của người dùng có thể đưa tới chủ của nó qua HTTP hoặc e-mail hoặc chuyển tới đĩa hoặc card thông minh để phân phối nhân công.

Các khoá riêng của mỗi cặp khoá chung được cấp phát sẽ lưu trữ bên trong một bộ nhớ trung tâm để được bảo mật tránh truy cập không hợp pháp. Các bộ nhớ này cũng nên được dự phòng trong mô hình bảo mật (như các tệp được mã hoá), vì nó là một phần của hệ thống hủy khoá nên cần thông báo lâu hơn để giải mã nếu khoá bị mất hoặc được thỏa hiệp và được hủy bỏ. Các băng dự phòng cần được đề phòng cẩn thận và đánh giá chính xác.

Khởi tạo
Bỏ đăng ký
Phục hồi
Người dùng đăng ký
Người dùng bỏ đăng ký
Tạo cặp khoá
Chứng nhận khoá công cộng
Chuẩn bị CRL
Lưu trữ khoá riêng
Lưu trữ chứng nhận
Lưu trữ CRL
Phục hồi khoá riêng
Phục hồi chứng nhận
Phục hồi CRL
Xác minh khoá công cộng
Xác minh chứng nhận
Sử dụng khoá riêng
Sử dụng khoá riêng
Biểu diễn khoá riêng
Biểu diễn chứng nhận

Hình 13.5: Tạo và kiểm tra một khoá công cộng

Vì bạn đang chỉ định tất cả các chứng nhận được cấp phát như một quyền đăng nhập chứng nhận, đặc biệt, trạm làm việc chuyên dùng cần được tổ chức để lưu trữ phương tiện định khoá riêng (như gọi chứng nhận gốc); đồng thời trạm làm việc này cũng sẽ bao hàm phần mềm (và bất kỳ phần cứng đặc biệt được yêu cầu) để tập hợp, chỉ định, phân tán và hủy bỏ các chứng nhận. Trạm làm việc này cũng nên bảo mật vật lý để ngăn cản quyền truy cập bất hợp pháp, nó không nên sử dụng như một máy tính đa mục đích.

Một trong những mục đích của các chứng nhận điện tử là để phối hợp cặp khoá chung, hệ thống chứng nhận tạo khoá chung để sẵn sàng khi cần. Phương thức thông dụng là lưu khoá chung trong một thư mục. Mặc dù các thư mục chủ/tớ lớn để các chứng nhận có cơ sở trên X.500 có dịch chuyển để sử dụng giao thức khác là LDAP (Lightweight Dierectory Access Protocol), sử dụng nhiều cấu trúc X.500, nhưng dựa trên TCP/IP. Bây giờ nhiều máy chủ chứng nhận đưa ra sử dụng tại các vị trí thống nhất đặt cơ sở trên LDAP. Sự gia tăng phổ biến của LDAP để truy cập thư mục giúp bạn liên kết các thư mục khác trên cơ sở các dịch vụ tới các chứng nhận điện tử của bạn.

Các máy chủ chứng nhận cũng duy trì và làm sẵn một danh sách hủy bỏ chứng nhận cho phép người dùng biết thời hạn các chứng nhận. Ví dụ các chứng nhận bị hủy bỏ vì bị mất, đánh cắp hoặc vì người làm thôi việc ở công ty.

Đối với số lượng nhỏ các chứng nhận điện tử, một máy chủ chứng nhận tập trung sẽ đáp ứng đủ nhu cầu. Nhưng, nếu số lượng chứng nhận mà công ty yêu cầu lớn, sử dụng nhiều máy chủ chứng nhận, xếp đặt theo phân loại của hệ thống (có cơ sở trên các công ty) sẽ dễ điều khiển và đáng tin cậy vì hệ thống không có hơn một điểm sự cố. Một số máy chủ chứng nhận hỗ trợ nhiều mức quản lý, cụ thể, một nhóm có thể có thể thực hiện phê chuẩn chứng nhận và các tác vụ hủy bỏ và một nhóm khác có thể thi hành các chức năng này như việc chỉ định quyền đăng nhập chứng nhận tới CA cấp dưới. Nó có thể tổ chức phân phối quản lý bằng việc chỉ định trách nhiệm cho một phần của cây thư mục tới CA khác và tập các bộ quản lý.

Bạn cũng có thể thiết lập các thông số cho các client từ hệ thống trung tâm của bạn. Các thông số này nên bao gồm các mặc định như máy chủ xác thực thư mục và những người chỉ định chứng nhận.

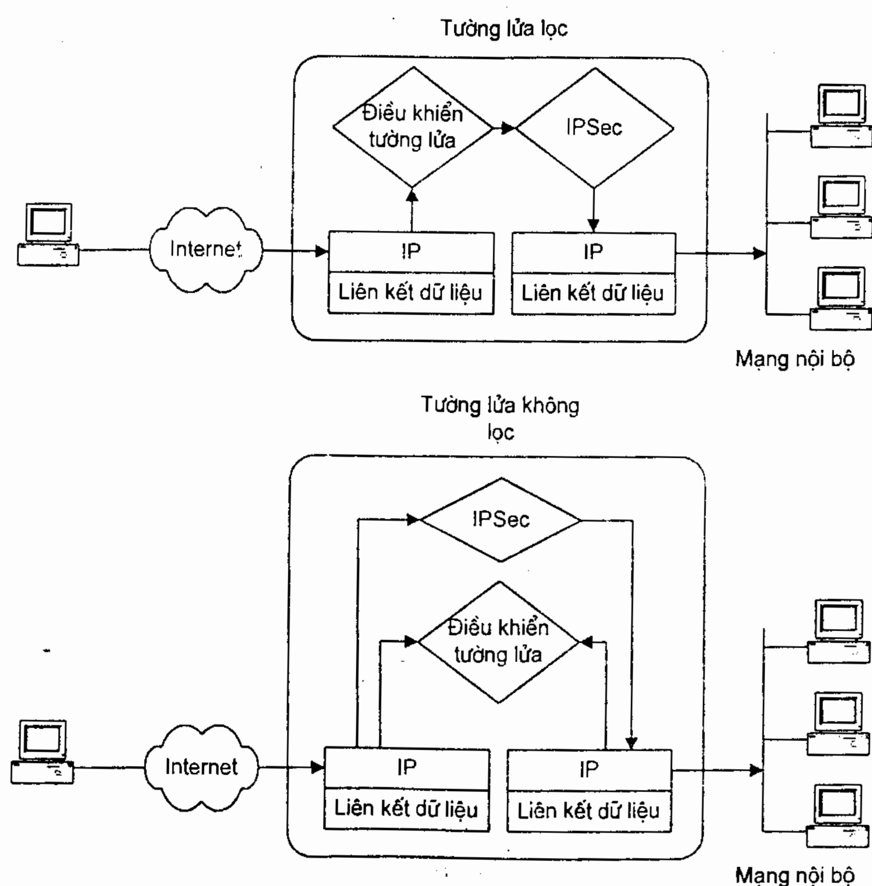
Tác vụ hỗ trợ người dùng truy cập các chứng nhận sẽ trở nên dễ hơn rất nhiều nếu hệ thống của bạn có thể hỗ trợ nhiều hơn một phương thức để được yêu cầu và được nhận một chứng nhận. Mức tối thiểu, các client có thể sử dụng HTTP, e-mail và các tệp trên đĩa để thực hiện công việc này. Các card thông minh cũng là phương tiện tốt để phân phối và lưu trữ các chứng nhận.

Bạn nên lưu và bảo mật các chứng nhận. Để chống mất cắp cần có một số yêu cầu để bảo mật chứng nhận.

Cuối cùng phần mềm cần cung cấp kiểm tra tự động hiệu lực của chứng nhận sử dụng CLR tải xuống (khi sử dụng ngoại tuyến). Khi OCSP trở nên sẵn có, xem các phần mềm hỗ trợ nó cho các chứng nhận có thể được kiểm tra trực tuyến một cách trực tiếp.

13.7 Điều khiển quyền truy cập

Một VPN được cấu tạo để cung cấp liên lạc giữa các host và các cổng nối bảo mật, có thể bạn vẫn muốn duy trì một vài điều khiển trên việc truy cập tới tài nguyên mạng của người dùng VPN. Cụ thể, nếu nhân viên bán hàng không được phép truy cập tới tài nguyên của nhóm nghiên cứu và phát triển (R&D) khi họ ở trên một LAN nối kết cứng, họ sẽ vẫn bị hạn chế từ chính truy cập nếu họ quay số trong VPN trong khi họ ở trên đường. Theo phương pháp này, bạn sẽ nhập điều khiển truy cập đường truyền mới được cung cấp bởi VPN với chương trình điều khiển truy cập hiện hành trong các bộ định tuyến và các tường lửa.



Hình 14.6: VPN lọc gói bằng tường lửa

Lưu lượng VPN có thể được điều khiển theo hai phương pháp khác nhau bằng một tường lửa không lọc các gói hoặc có lọc các gói (xem hình 13.6). Trong phương pháp không lọc, lưu lượng VPN được điều khiển trong cùng một bộ định tuyến, giúp cho dữ liệu bảo mật được dịch chuyển trực tiếp tới mạng nội tại không cần lọc và điều khiển trên nội dung của nó. Trong phương pháp lọc, điều

khiển ủy quyền và lọc của tường lửa được thực hiện tới lưu lượng của VPN trước khi nó được phép bên trong mạng nội tại. Việc lọc lưu lượng VPN có thể hữu ích rõ rệt nếu chính sách bảo mật qua các kiểu lưu lượng xác thực nhất giữa các vị trí VPN, như e-mail và FTP. Việc lọc cũng có thể hữu ích đối với việc điều khiển lưu lượng thay đổi với các đối tác kinh doanh nếu bạn mở rộng VPN tới một Extranet.

Nếu vị trí cổng nối ở giữa Internet và một bộ định tuyến (và các tường lửa theo sau) có thể được dùng để lọc cả lưu lượng không-VPN và VPN với cùng các chỉ dẫn; cổng nối sẽ cung cấp các dịch vụ mã hoá và giải mã trong suốt tới mọi vị trí. Vậy bộ định tuyến không cần phải cấu hình lại để cho qua đường hầm lưu lượng đặc biệt, đây là trường hợp khi cổng nối được thiết lập sau bộ định tuyến. Khuyến cáo: nếu cổng nối chung hoặc không tin cậy, bạn cần đảm bảo chính quản lý cổng nối có thể không được thỏa thuận từ vài người trên mạng không tin cậy. Nếu kết nối này đang điều khiển cả lưu lượng không-VPN và VPN, khi đó cổng nối VPN cần được cấu hình để cho qua lưu lượng không-VPN.

Khi cổng nối định vị sau một bộ định tuyến và tường lửa, thiết bị điều khiển sẽ có được cấu hình để cho qua lưu lượng VPN không lọc. Mặc dù tăng độ bảo mật của cổng nối (cụ thể nó không dễ bị ảnh hưởng đối với quản lý cổng được thỏa thuận) cho thấy bạn ít điều khiển trên lưu lượng của LAN đang nhập sau khi giải mã bởi cổng nối. Nếu bạn muốn lọc lưu lượng VPN bởi đích, cụ thể kiểu TOD hoặc kiểu ứng dụng, khi đó bạn có lọc nhân bản từ bộ định tuyến hoặc tường lửa trên cổng nối.

Tổng kết

Có nhiều quản lý bảo mật cho VPN là mở rộng đơn giản các chính sách bảo mật thống nhất chuẩn, đặc biệt đối với xác thực của những người dùng và điều khiển truy cập của họ tới các tài nguyên mạng. Dĩ nhiên, VPN đòi hỏi bổ sung sự hiểu biết các thành viên, sự mềm dẻo của các nguyên tắc mã hoá khác nhau và liên kết các chiều dài khoá để truyền dữ liệu trên một VPN được bảo mật hoàn toàn.

Phân phối các khoá để xác thực các cổng nối bảo mật và các host từ xa trên một VPN là phần quan trọng của việc quản lý VPN, với nhiều hệ thống dùng các chứng nhận điện tử cho tác vụ này. Các quyền đăng nhập chứng nhận thương mại hoặc máy chủ chứng nhận nội bộ riêng có thể được sử dụng để cấp phát và điều khiển các chứng nhận điện tử.

CHƯƠNG 14

QUẢN LÝ ĐỊA CHỈ IP

Sự phát triển bùng nổ trong việc sử dụng IP để truyền thông dữ liệu, kể cả ở các bộ phận kỹ thuật và các tổ chức thương mại có chỉ dẫn một số vấn đề về việc cấp phát và quản lý các địa chỉ IP. Mặc dù không gian địa chỉ gốc 32 bit của IPv4 có thể xem như đầy đủ để điều khiển bất kỳ yêu cầu nào của mạng khi nó được mô tả lần đầu tiên, không gian địa chỉ IPv4 sẽ nhanh chóng không đủ cung cấp tại mức tối thiểu cho Internet chung (bạn sẽ xem vắn tắt về mạng liên kết riêng ở nội dung khác). Phiên bản 6 hoặc IPv6 là phiên bản tiếp theo của IP, có các đặc tính là một không gian địa chỉ 128 bit, sẽ được áp dụng trong tương lai, nhưng cho đến khi nó được triển khai rộng rãi, các giải pháp ngắn hạn đã được sử dụng để giải quyết sự thiếu hụt về địa chỉ. Các giải pháp ngắn hạn giúp mạng quản lý phân phối định tuyến và lập địa chỉ, chúng có thể đưa ra giải pháp để triển khai VPN.

Mặc dù IPSec cũng như nhiều giao thức khác, có thể thích hợp nhất cho việc sử dụng với IPv6, phần lớn chúng phải phân phối với vùng phụ cận hiện hành, tiếp tục sử dụng IPv4 và bổ sung tính phức tạp do chính các giải pháp ngắn hạn khác nhau mang đến với nó. Vì IPv4 tiếp tục sử dụng phổ biến trong một vài năm tiếp theo nên sự triển khai và thiết kế VPN thích hợp với quản lý địa chỉ phụ cận có tính phức tạp khi mạng điều khiển hướng về các giải pháp khác, điều đó sẽ làm cho việc lập địa chỉ để sử dụng trong VPN dễ hơn.

Chương này chỉ ra một vài vấn đề trợ giúp người quản lý và người thiết kế, bao trùm các phương thức hiện hành để cấp phát các địa chỉ tới các thiết bị mạng, trên cả các mạng riêng và chung, giống như tác vụ liên quan việc đặt tên các thực thể mạng qua dịch vụ tên miền DNS (Domain Name Service). Tiếp theo chúng ta đưa ra một vài vấn đề đặc biệt mà VPN có thể gặp phải. Bất cứ ở đâu chúng ta cũng có thể thảo luận để đưa ra các giải pháp hiện hành giải quyết các vấn đề này.

14.1 Cấp phát địa chỉ và các dịch vụ đặt tên

Trong các tổ chức thương mại lớn, việc cấp phát các địa chỉ IP giữa hàng ngàn các trạm làm việc và cấu hình các địa chỉ này trong phần mềm TCP/IP thường là một tác vụ khó. Trước kia, bổ sung, di chuyển hoặc thay đổi các trạm làm việc và các máy chủ yêu cầu phân bố nhân công một địa chỉ IP mới. Phương pháp đơn giản để kiểm tra các địa chỉ, như cuốn sổ tay hoặc bảng tính điện tử, có thể làm đối với các mạng nhỏ, nhưng phương pháp này nhanh chóng trở nên quá tải khi các mạng bắt đầu lớn hơn. Các máy chủ tự động và các công cụ liên quan được triển khai để đảm bảo mạng chạy trơn tru. Trước hết, ở giữa các mạng IP này là giao thức điều khiển host động DHCP (Dynamic Host Control Protocol) cho việc quản lý địa chỉ và DNS cho quản lý tên và bây giờ, sử dụng DNS động (Dynamic DNS) liên kết hai kiểu quản lý mạng sẽ dễ hơn, mặc dù không dễ điều hành.

Một vấn đề khác do việc chỉ định không đủ các địa chỉ mạng. Không có chỉ định riêng biệt, các địa chỉ có thể bị mất trong khi thay đổi thiết bị hoặc khi vừa mới di chuyển, khi đó phát triển mạng sẽ dẫn đến khan hiếm địa chỉ. Đôi khi có việc chỉ định sai lầm, cùng một địa chỉ tới hai máy khác nhau, điều này có thể dẫn tới việc mất kết nối và định tuyến.

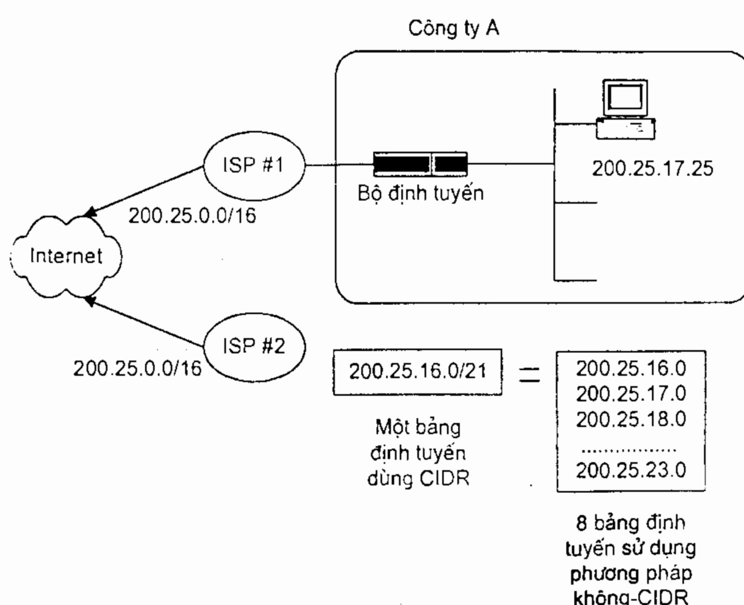
Một tác vụ khó khác là các địa chỉ cấp phát cho những người dùng di động. Người bán không có văn phòng riêng với các máy tính xách tay có thể được cung cấp với các địa chỉ đa mạng, một bộ định tuyến hoặc một máy chủ truy cập từ xa, chúng truy cập qua một kết nối quay số dẫn tới việc mất các địa chỉ và việc kiểm tra trở nên khó khăn. Đa địa chỉ là không cần thiết khi bạn chuyển đổi các người dùng của các máy chủ truy cập từ xa tới một VPN, nhưng bạn có thể vẫn muốn chỉ định địa chỉ một cách linh động hơn là sử dụng cấp phát tĩnh.

Trạng thái hiện tại của các địa chỉ được cấp phát tới các công ty cũng gây ra nhiều vấn đề. Các công ty yêu cầu các địa chỉ cho hơn 1000 thiết bị không thể lấy địa chỉ mạng lớp A hoặc B và thường bắt buộc sử dụng định tuyến liên miền không phân lớp CIDR (Classless Inter-Domain Routing) để kết hợp các địa chỉ lớp C sẵn có. Nhưng, sử dụng CIDR yêu cầu các số mạng gần kề, để đưa tới các mạng nhóm bởi vùng, do vậy tất cả các số mạng bên trong vùng đã cho có thể mô tả bằng một lối vào duy nhất trong bảng định tuyến của các vùng khác nhau (xem hình 14.1).

Nếu các địa chỉ cho các thiết bị trong một vùng đã cho không được cấp phát gần kề, khi ấy bảng định tuyến có thể không thực hiện được và chất lượng bộ định tuyến sẽ giảm.

14.1.1 Cấp phát địa chỉ động và tĩnh

Trong phần trước, một địa chỉ IP thường được cấp phát nhân công tới một thiết bị mạng như một bộ định tuyến, máy chủ hoặc một trạm làm việc khi thiết bị tác động tới mạng (các máy in và các thiết bị sử dụng BOOTP bị loại ra). Cụ thể các thiết bị này phù hợp trong các mạng con mà thiết bị được định vị là 172.52.X.X cho các phòng nhân sự (Human Resources) đối lập với 172.53.X.X cho phòng nghiên cứu và phát triển (R&D) và có thay đổi nếu máy tính định vị lại đến mạng con khác. Hỗ trợ hơn nữa, một địa chỉ của thiết bị là tĩnh và không thay đổi nếu không có một ai (thường là người quản trị mạng) thay đổi tệp cấu hình của thiết bị.



Hình 14.1: CIDR và tập các bảng định tuyến

Cấp phát các địa chỉ IPv4

Các địa chỉ IPv4 được phân bố trong 3 lớp chính: A, B và C (lớp thứ tư D được dự trữ cho các sử dụng đặc biệt giống như đa phương tiện). Mỗi địa chỉ bao gồm 4 octet (mỗi octet = 8 bit), tổ chức bởi 8 số nhị phân hoặc phân ra các số thập phân. Octet đầu tiên được dùng để định danh lớp địa chỉ IP. Các địa chỉ lớp A sử dụng 3 octet cuối cho các nút IP cụ thể; các địa chỉ lớp B sử dụng 2 octet cuối cho mục đích này; và các địa chỉ lớp C sử dụng octet cuối.

Địa chỉ mạng lớp A là đáng giá nhất, bởi vì chúng đủ lớn để để phục vụ các nhu cầu của các tổ chức thương mại với kích thước bất kỳ (xem bảng 14.1). Nhưng vì có ít hơn 128 mạng lớp A tồn tại trong toàn bộ Internet, như vậy sẽ rất

hiếm và không có nhiều mạng lớp A hơn để cấp phát. Chỉ những tổ chức sớm sử dụng Internet (Xerox Corp, Stanford U, BBN) mới được quyền sở hữu các mạng lớp A.

Bảng 14.1 Các tài nguyên của các lớp địa chỉ IPv4

Lớp	ID mạng	Số mạng	ID địa chỉ trạm	Số trạm
A	7 bit	128	24 bit	16.777.216
B	14 bit	>16.000	16 bit	65.536
C	21 bit	>2.000.000	8 bit	256

Lớp B có hơn 16.000 mạng cũng trở nên khan hiếm và bây giờ cũng khó thu được. Các địa chỉ mạng lớp C cung cấp lớn hơn (trên 2.000.000) do vậy chúng vẫn dư thừa. Vấn đề chủ yếu cho phần lớn các tổ chức là mạng lớp C nhỏ (một mạng chỉ chứa được tối đa 256 địa chỉ). Ngay cả với một mạng lớp B cũng không đủ lớn cho một tổ chức thương mại với hơn 1.000 mạng LAN.

Tuy nhiên ở các mạng tĩnh đầu xa thì thiết bị được thay đổi hoặc được cung cấp; con người và thiết bị được di chuyển và kiến trúc lại các mạng. Chỉ định nhân công các địa chỉ IP tĩnh tiêu tốn nhiều thời gian khi có bất cứ một thay đổi cần thiết, nó cũng có thể là một quá trình hay sai lỗi. Để giải quyết vấn đề này cần đưa ra một phương thức động để cấp phát các địa chỉ, đó là DHCP (Dynamic Host Control Protocol) được triển khai. Và, do các người dùng quen dùng và nhớ tên dễ hơn là các địa chỉ cho các thiết bị mạng, dịch vụ đặt tên chuẩn DNS (Domain name service) cũng được cải tiến để nó có thể liên kết linh hoạt với DHCP và kiểm tra bất kỳ thay đổi bởi DHCP.

DHCP được thiết kế để cung cấp một phương pháp tập trung tới cấu hình và duy trì một không gian địa chỉ IP, mạng quản lý cấu hình các loại thiết bị trên mạng được định vị duy nhất. DHCP cho phép các địa chỉ IP được chỉ định linh động tới các trạm làm việc, loại trừ nhu cầu cấp phát địa chỉ IP tĩnh bởi mạng và bộ tham mưu quản lý các hệ thống. Các máy chủ DHCP giúp các địa chỉ IP sẵn có được duy trì.

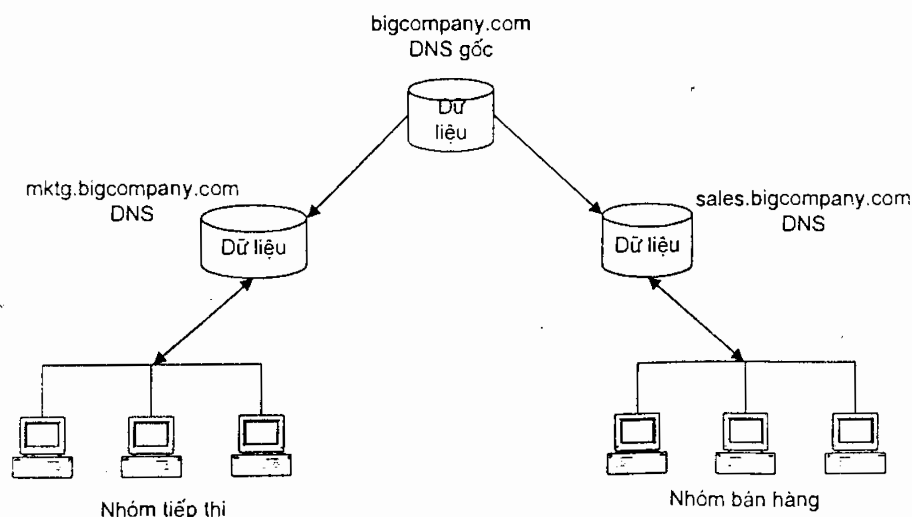
Hoạt động DHCP hoàn toàn đơn giản. Khi một trạm làm việc client DHCP nạp hệ điều hành, nó truyền thông một yêu cầu DHCP cho bất kỳ một máy chủ DHCP trên mạng để cung cấp cho nó một địa chỉ IP và các thông số cấu hình. Một máy chủ DHCP trên mạng được tác quyền để cấu hình client này sẽ đưa ra một địa chỉ IP bằng việc gửi một phúc đáp tới client. Client có thể chấp nhận nó

hoặc đợi đưa ra thêm từ các máy chủ khác trên mạng. Cuối cùng, client chọn lọc đưa ra công bố chi tiết đến máy chủ thích hợp. Máy chủ được chọn lọc khi đó sẽ gửi trả báo nhận với địa chỉ IP được đưa ra và bất kỳ một thông số cấu hình khác mà chính client yêu cầu.

Máy chủ DHCP không hạn chế việc chỉ định các địa chỉ động duy nhất. Tập các địa chỉ có thể lập để dành như các địa chỉ mạng tĩnh cho việc chỉ định tới các client đặc biệt, giống như các máy chủ dịch vụ tệp và thư điện tử. Máy chủ DHCP cho phép thời gian tồn tại các địa chỉ tĩnh là vô hạn.

Địa chỉ IP đưa tới client bởi máy chủ DHCP có thoả thuận về thời gian tồn tại, điều này chỉ thị địa chỉ IP có hiệu lực bao lâu. Trong suốt thời gian sống của địa chỉ động, client sẽ thường xuyên hỏi máy chủ để tái lập. Nếu client không muốn tái lập hoặc máy client kết thúc địa chỉ IP này có thể đưa đến máy khác.

Dịch vụ tên miền DNS là hệ thống đặt tên chính thức của Internet và được thiết kế sao cho tên các tài nguyên mạng khác nhau, gồm cả địa chỉ IP. DNS là hệ thống đặt tên phân tán, cơ sở dữ liệu là các tên tịnh tiến để các đối tượng được rải ra qua hàng ngàn máy tính.



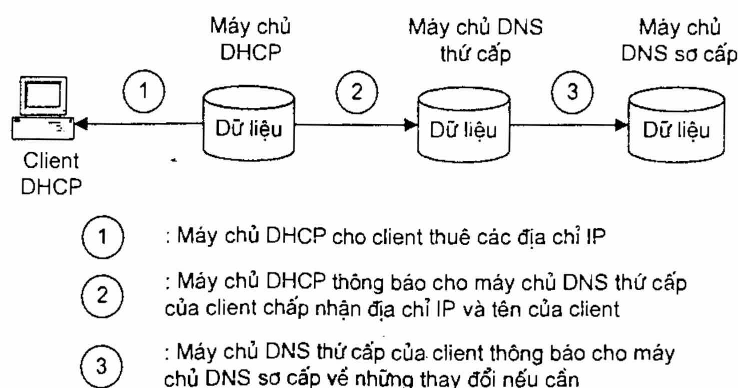
Hình 14.2: Kiến trúc của các máy chủ DNS

Các yêu cầu tên miền (yêu cầu để sửa đổi tên mạng trong địa chỉ mạng tương quan của nó) được điều khiển bởi kiến trúc các máy chủ DNS (xem hình 14.2). Các yêu cầu được gửi đầu tiên tới máy chủ tên cục bộ trong kiến trúc mạng với địa chỉ IP của máy chủ tên này cấu hình đặc trưng trong mỗi phần mềm TCP/IP của trạm làm việc. Nếu máy chủ tên này không trả lời được chất vấn, nó

gửi yêu cầu tới máy chủ tên mức cao hơn. Máy chủ tên mức cao hơn có thể phân tích tự động các yêu cầu tên hoặc thu thông tin từ trạm máy chủ tên mức thấp hơn khi không biết tới yêu cầu gốc. Ví dụ, nhóm tiếp thị và bán hàng trong các miền con tại công ty lớn (bigcompany.com) có thể có máy chủ tên tại cùng một mức trong hệ thống DNS, nhưng cách duy nhất để các người dùng trong tiếp thị có thể thu thông tin từ bán hàng là máy chủ tên sẽ yêu cầu qua thiết bị COM của máy chủ tên mức cao hơn.

Trước đây, DNS được thiết kế để làm việc với địa chỉ IP tĩnh. Một đặc tính quan hệ mới là DNS động (DDNS) được định nghĩa bởi IETF (RFC 2136) và bây giờ được cung cấp bởi các nhà cung cấp cho các máy chủ DHCP một cách tự động qua thông tin chỉ định hợp đồng địa chỉ IP tới các máy chủ DNS. cho phép các trạm làm việc với các địa chỉ được chỉ định linh động bởi DHCP được máy chủ DNS theo dõi; các trạm làm việc sau đó được đưa ra bởi một tên mà không cần duy trì nhân công cơ sở dữ liệu DNS (xem hình 14.3).

Thậm chí qua DHCP và DNS động có thể quản lý địa chỉ IP dễ dàng, cấp phát các địa chỉ IP động của DHCP có thể gây ra một số vấn đề khác. Một vài tường lửa và các sản phẩm bảo mật Internet khác theo dõi các địa chỉ IP trên chiếm giữ để một địa chỉ duy nhất nhận dạng một máy tính. Nếu các sản phẩm này có thể không được ánh xạ trở lại địa chỉ DHCP chỉ định tới một người dùng đặc biệt, một người dùng bất hợp pháp có thể truy cập lại tới mạng vì địa chỉ được tác quyền đi ngoài tầm tường lửa mà không biết.



Hình 14.3: Ghép DHCP và DNS động

Tương tự, bất kỳ động tác để gỡ rối các vấn đề trên một mạng hoạt động tin cậy ở trên có thể tịnh tiến một địa chỉ IP tới máy tính riêng. Các vấn đề khác có thể xảy ra từ chính chỉ định địa chỉ IP động bao gồm điều khiển dung lượng lọc (hạn chế xem nội dung Web ở một vài vị trí nào đó) giống như một danh sách.

Phân bố các địa chỉ động có thể phát sinh các vấn đề đối với việc cài đặt bảo mật. Bởi vì, các tường lửa thường tương thích quyền truy cập tới các địa chỉ IP, các hệ thống hỗ trợ DHCP sẽ cho phép phần đặt trước của một tập địa chỉ IP cho một nhóm người dùng (cụ thể là một ban hoặc một tổ chức tên đặc biệt). Sử dụng các tường lửa có thể điều khiển trên một nhóm cơ bản khi các địa chỉ IP được chỉ định một cách linh động.

Mặc dù DHCP thích hợp với DDNS, nhưng có thể sử dụng DHCP mà không cần DDNS. Trong trường hợp, không phải tất cả các thiết bị trên mạng có địa chỉ được chỉ định linh động. Khi chỉ định các địa chỉ IP tới các máy chủ tệp tin, e-mail và các máy chủ quan trọng khác trên mạng, nên sử dụng việc chỉ định địa chỉ tĩnh. Cách này có thể sử dụng DNS ánh xạ trực tiếp các tên mạng tới các địa chỉ mạng. Tương tự, các trạm làm việc đó đảm nhận khả năng làm việc cũng cần các địa chỉ tĩnh do vậy chúng được DNS kiểm tra.

14.1.2 Đối lập giữa DNS bên trong và bên ngoài

Khi bạn đang bảo mật truy cập từ bên ngoài tới Extranet giao tiếp với một tường lửa hoặc một cổng nối bảo mật, có một số bước liên quan để bảo mật dịch vụ tên miền trong khi vẫn cho phép người dùng truy cập các tài nguyên ở bên ngoài khi cần thiết (và được phép). Điều này thường đòi hỏi việc thiết lập phối hợp giữa hai DNS.

Đối với một mạng IP riêng, máy chủ DNS thống nhất sẽ đáp ứng, bởi vì nó có thể cất giữ một cách cẩn thận tất cả các phép tịnh tiến tên-địa chỉ cho mạng và không có một kết nối tới Internet chung để giúp những người ngoài duy trì từ các tên được phát minh của các tài nguyên được đánh giá thống nhất.

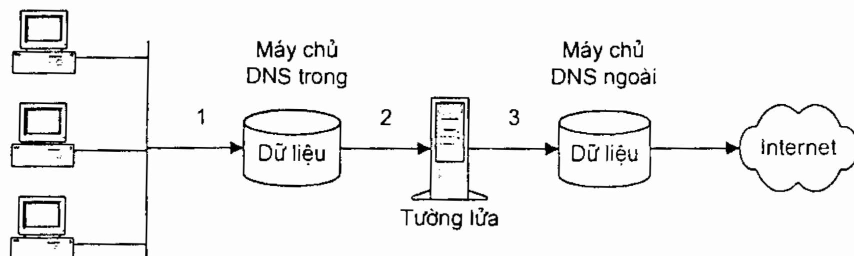
Vấn đề đầu tiên xảy ra khi có một kết nối tới Internet và dùng các nhu cầu truy cập tới các nguồn tài nguyên ở bên ngoài. Để các tên ánh xạ đúng tới các địa chỉ, máy chủ DNS bên trong liên lạc với một máy chủ DNS bên ngoài. Nhưng, do không muốn người dùng bên ngoài truy cập tới tài nguyên bên trong, do vậy cần phải bảo mật máy chủ DNS bên trong (dọc theo các nguồn tài nguyên mạng khác), vậy phải thiết lập một tường lửa. Vì máy chủ DNS của ISP ở bên ngoài tường lửa và máy chủ DNS của bạn ở bên trong tường lửa nên chúng có thể không sẵn sàng liên lạc để truy cập các nguồn tài nguyên bên ngoài.

Giải pháp là thiết lập hai máy chủ DNS thống nhất: một ở bên ngoài tường lửa và một ở bên trong tường lửa. Đây là phối hợp hai DNS. Bước tiếp theo là phân chia các host đã có trên máy chủ DNS nền trong hai nhóm. Các host này trong nhóm danh sách đầu tiên mà bất kỳ một ai trên Internet tìm được như e-mail cổng nối, các Web site công cộng và máy chủ FTP vô danh. Cụ thể, nó cũng

bao hàm tên giao tiếp bên ngoài tường lửa. Danh sách thứ hai chứa tập các host mà chỉ các người dùng mạng bên trong mới được tìm kiếm. Không quên rằng, danh sách thứ hai cũng sẽ bao hàm các host bên ngoài để người dùng bên trong có thể tìm kiếm.

Do yêu cầu, máy chủ DNS bên ngoài lưu trữ danh sách đầu và máy chủ DNS bên trong lưu trữ danh sách thứ hai. Các máy chủ DNS bên ngoài được báo tới Internet khi máy chủ DNS đáng tin cậy cho miền mà các phương cách để yêu cầu từ các host trên nền Internet sẽ đưa đến máy chủ DNS bên ngoài, nhưng không đưa đến máy chủ DNS bên trong.

Các host trên mạng bên trong sử dụng máy chủ DNS bên trong như máy chủ DNS chính. Khi muốn truy cập các host bên ngoài, máy chủ DNS bên trong sẽ đưa ra các yêu cầu về tên miền DNS tới máy chủ DNS bên ngoài ở bên ngoài tường lửa. Điều này được hoàn thành bởi máy chủ DNS bên trong sẽ được cấu hình với một thực thể chuyển tiếp, nó có tác dụng tìm kiếm máy chủ DNS bên ngoài ở mọi nơi. Vì các yêu cầu qua tường lửa nên một dịch vụ uỷ quyền DNS được cài đặt trên tường lửa, nó cho phép phân biệt kết nối tới máy chủ DNS bên ngoài trên sự thay mặt của máy chủ DNS bên trong (xem hình 14.4).



Hình 14.4: Liên kết DNS trong và ngoài

Các tình huống tương tự có thể gặp phải với VPN. Nếu sử dụng một máy chủ DNS và bảo mật các lối vào DNS từ phần còn lại của thế giới, khi đó sẽ cần một phương pháp để cung cấp các thông tin này tới các vị trí khác và các người dùng từ xa của VPN để họ có thể hoàn thành các kết nối tới các tài nguyên thích hợp. Nếu có ý định cho phép truy cập tới một số hữu hạn các host trên VPN, khi đó cần duy trì gấp đôi các lối vào DNS, một tập tin chứa các thói quen bên trong và thứ hai cho VPN sử dụng.

14.2 NAT và các địa chỉ riêng

Các khối địa chỉ IP được cấp phát bởi IANA được chỉ định để sử dụng trên Internet chung. Nếu công ty không có mục đích sử dụng Internet mà chỉ truyền

lưu lượng IP trên mạng liên kết riêng của nó, khi đó bất kỳ một dải địa chỉ nào cũng có thể được sử dụng. Ngay sau đó, IETF khuyến nghị để chỉ các dải xác định được sử dụng do vậy các bộ định tuyến Internet sẽ không bị lầm lẫn nếu các địa chỉ được cho biết ngẫu nhiên trên Internet. Các khối này đã được định nghĩa trong RFC 1597 "*Cấp phát địa chỉ cho các mạng con riêng*" như sau:

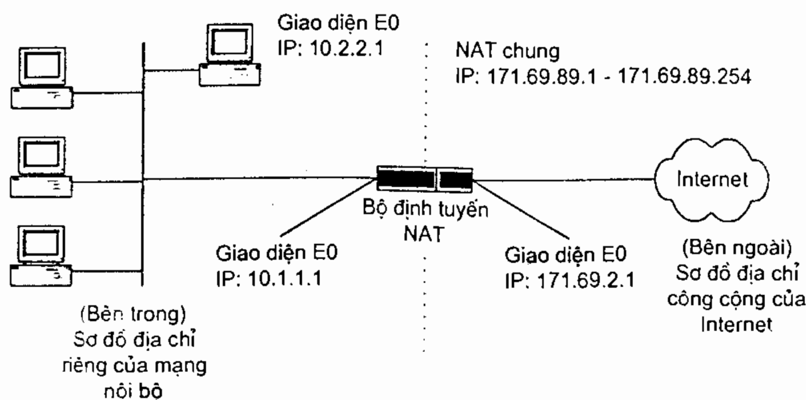
- Lớp A: 10.0.0.0 - 10.255.255.255.
- Lớp B: 172.16.0.0 - 172.31.255.255.
- Lớp C: 192.168.0.0 - 192.168.255.255.

Có có thể sử dụng các địa chỉ riêng này cho một mạng liên kết bên trong và vẫn kết nối tới Internet. Để làm được vậy, bạn cần được cấp phát một khối các địa chỉ đăng kiểm và sử dụng tường lửa hoặc bộ định tuyến để thực hiện phép dịch địa chỉ mạng NAT (Network Address Translation)

NAT sửa đổi phân phối địa chỉ bên trong với độ ưu tiên các địa chỉ đăng kiểm để đưa các gói tới Internet chung. Phép tịnh tiến có thể thích hợp với các đặc tính và khả năng định tuyến chuẩn. NAT cần áp dụng chỉ trên bộ định tuyến và tường lửa để được kết nối vật lý đến phối hợp lập địa chỉ bên ngoài và bên trong.

NAT là giao tiếp độc lập, điều đó chỉ ra rằng NAT có thể áp dụng tới bất kỳ giao tiếp nào trên bộ định tuyến để liên kết các phối hợp lập địa chỉ bên trong tới bên ngoài.

Trong hình 14.5, hệ thống host sử dụng một địa chỉ IP riêng là 10.2.2.1 như một phần của Intranet. Khi gói đưa đến bộ định tuyến, NAT dịch địa chỉ 10.2.2.1 vào bên trong địa chỉ khác từ vùng chứa NAT IP cấp phát, cho là 171.69.89.2. Nó giống như các máy được di chuyển ảo tới đoạn mạng bên ngoài cho các mục đích truyền thông bên ngoài. Đây là đoạn mạng ở trong một hộp bộ chỉ đường NAT tự động cho ví dụ này.



Hình 14.5: NAT tại bộ định tuyến biên

Khi cần phối hợp lập địa chỉ bên ngoài thì mới cần quan tâm đến vùng chứa NAT IP, còn khi lập địa chỉ bên trong thì không cần.

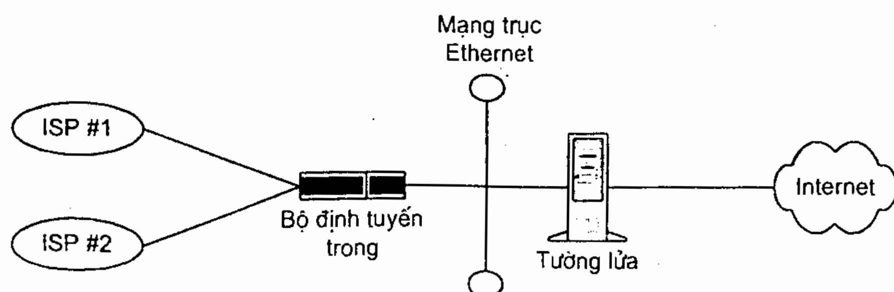
Nên nhớ rằng NAT yêu cầu khả năng truyền bất kỳ một phần nào của các tiêu đề và các gói để liên hệ phối hợp lập địa chỉ. IP và TCP tổng kiểm tra nhu cầu có thể truy cập, giới hạn mã hoá của các miền này. Khi dữ liệu được mã hoá bên trong các gói IP, nó không thể làm được cho NAT để thực hiện tịnh tiến địa chỉ bên trong gói. Như vậy, các host sử dụng mã hoá nên chỉ định đăng kiểm hợp pháp, các địa chỉ bên ngoài được miễn ở NAT.

Một bất lợi quan trọng là việc mất vết IP từ đầu cuối đến đầu cuối. Nó trở nên khó khăn để tìm ra các gói do gói thay đổi qua nhiều NAT.

Nếu một tổ chức thương mại sử dụng không gian địa chỉ riêng, khi ấy các client DNS bên ngoài tổ chức sẽ không thấy các địa chỉ bên trong, bởi vì các địa chỉ này không rõ ràng. Một cách để đảm bảo đó là hoạt động trên hai máy chủ cho mỗi vùng DNS chứa địa chỉ các host chung và riêng. Một máy chủ có thể thấy từ không gian địa chỉ chung và sẽ chỉ chứa mạng con gồm các địa chỉ của tổ chức thương mại, chính điều này có thể đưa đến việc sử dụng địa chỉ chung. Máy chủ khác sẽ chỉ được đưa đến từ mạng riêng và sẽ chứa đầy đủ tập dữ liệu, bao gồm cả các địa chỉ riêng và bất kỳ địa chỉ chung nào được đưa đến từ mạng riêng.

Cấu hình NAT có thể trở nên đặc biệt phức tạp đối với VPN, do vậy nhiều nhóm làm việc khác nhau bên trong IETF vẫn xem xét việc sử dụng đặc thù của NAT là giải pháp tốt nhất và chúng sẽ ảnh hưởng đến việc thiết kế VPN như thế nào?

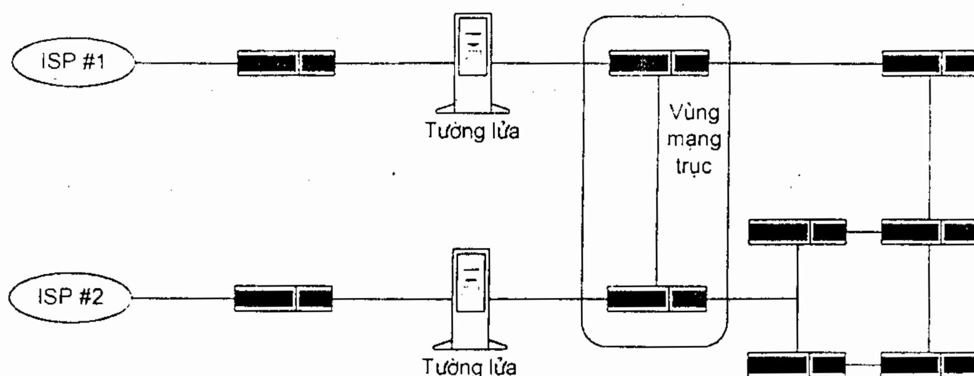
14.3 Đa liên kết tới Internet



Hình 14.6: Kết nối nhiều vị trí đến 2 ISP

Nếu bạn muốn tăng độ tin cậy của các kết nối Internet cho một VPN, phương pháp đầu tiên là sử dụng các kết nối Internet dư thừa (2 hoặc nhiều hơn các kết nối đang duy trì) các kết nối do các ISP khác nhau phục vụ. Nhưng, các kết nối dư thừa phải xem xét các vấn đề của riêng chúng khi cấu hình các tường lửa và các bộ định tuyến.

Phương thức đơn giản nhất để hỗ trợ một kết nối Internet thứ cấp là kết nối cả hai liên kết trên cùng một bộ định tuyến và sử dụng giao thức cổng nối biên BGP (Border Gateway Protocol) trên bộ định tuyến để phân xử ISP nào sẽ nhận lưu lượng (xem hình 14.6). Giải pháp này không có độ tin cậy cao nhất, bởi vì giống như bộ định tuyến (điều khiển BGP được gọi) có thể là một điểm duy nhất của sự cố. Để tăng độ tin cậy cần phân biệt hai tuyến tới các ISP, với các bộ định tuyến và các tường lửa phân biệt cho mỗi đường dẫn, như trong hình 14.7.



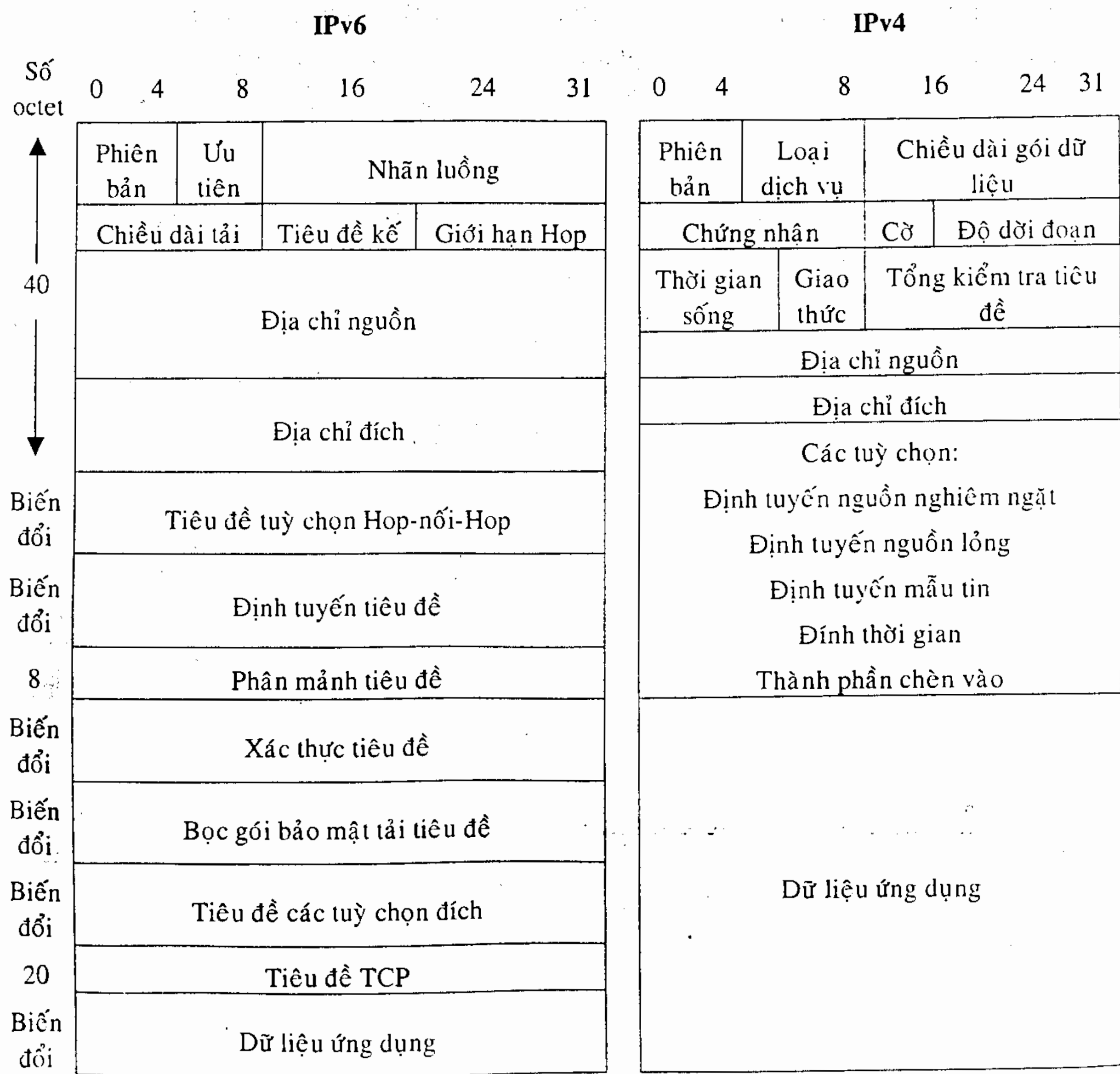
Hình 14.7: Kết nối nhiều vị trí sử dụng nhiều bộ định tuyến và BGP

Dĩ nhiên đây không phải là giải pháp lý tưởng. Với cấu hình này, vấn đề chính là phần lớn các tường lửa không chia sẻ thông tin về các kết nối; nếu kết nối thứ nhất có một điểm bị lỗi, thông tin về các phiên sử dụng có thể không qua thường xuyên trên các điểm của kết nối thứ hai để mà thông tin có thể tìm lại được tại điểm kết nối thứ hai. Phần lớn các cổng nối bảo mật hoạt động tương tự trên, tuy nhiên có ít nhất một sản phẩm như Contivity Extranet Switch của hãng Bay network có một hệ thống miễn lỗi (failover) cung cấp liên lạc giữa các máy chủ.

Nếu các cổng nối bảo mật và các tường lửa có cơ chế lọc gói đơn giản hoặc có thể chia sẻ thiết lập, bạn có thể sử dụng hai bộ định tuyến và các tường lửa để kết nối đến Internet nhằm cung cấp cho các host đã được đăng ký địa chỉ IP có thể liên lạc với Internet. Nếu bạn sử dụng các địa chỉ riêng kèm với việc dịch địa chỉ mạng (NAT) sẽ không thực hiện được việc kết nối đến Internet.

14.4 IPv6

Phiên bản hiện nay của IP là IPv4 và thế hệ tiếp theo của nó là IPv6. Kích thước địa chỉ IPv4 là 32 bit, cung cấp được 4.294.967.296 địa chỉ. Mặc dù nó đủ với giao thức được tạo đầu tiên năm 1978, thấy được không gian địa chỉ sẵn có. Một phương thức liên kết lớp đối với các khối địa chỉ được cấp phát - khối gần kề được chỉ định của các địa chỉ lớp A, B và C, các mạng dễ thực hiện nhưng không đạt hiệu quả phân phối địa chỉ, đặc biệt đối với các mạng vừa và nhỏ, CIDR được sử dụng để cấp phát địa chỉ có hiệu quả hơn.



Hình 14.8: Minh hoạ cấu trúc các gói IPv4 và IPv6

IPv6 đảm bảo cung cấp địa chỉ có hiệu quả. Điểm khác biệt đầu tiên giữa IPv4 và IPv6 là chiều dài trường địa chỉ. Trường địa chỉ của IPv6 dài 128 bit bằng bốn lần chiều dài trường địa chỉ của IPv4. IPv6 gồm cả việc hỗ trợ xây dựng đa phương tiện, IPSec và điều khiển luồng đối với chất lượng dịch vụ, những vấn đề trên cũng đã được hỗ trợ trong IPv4 nhưng đạt hiệu quả không cao bằng.

Vậy, tiêu đề IPv6 lớn hơn của IPv4, có ít trường hơn, điều đó sẽ giúp định tuyến có hiệu quả hơn vì các bộ định tuyến sẽ ít phải xử lý trên mỗi tiêu đề (xem hình 14.8).

Các địa chỉ 32 bit của IPv4 được chia vào trong bốn nhóm, một nhóm 8 bit gọi là các octet. Thiết kế IPv6 chọn định dạng tương tự gồm 8 số nguyên 16 bit phân cách nhau bởi dấu hai chấm. Một số nguyên được mô tả bởi 4 số hexa:

FEDC:BA98:7654:3210:FEDE:BA98:7655:2130

Các địa chỉ IPv6 tác động về mọi phần của mạng; không chỉ nâng cấp các ngăn xếp IP cho các máy tính client và host mà còn nâng cấp máy chủ DNS và bộ định tuyến. Máy chủ DNS được ráp lại với phần mềm có thể điều khiển địa chỉ IP lớn hơn, điều đó làm đơn giản việc mở rộng DNS. Nhưng việc chuyển dịch tới IPv6 sẽ cho phép bạn tạo phối hợp lập địa chỉ toàn cầu để tất cả các vị trí VPN không cần áp dụng NAT và do đó giảm nhu cầu tái cấu hình của các tường lửa và máy chủ DNS.

Tổng kết

Việc cấp phát địa chỉ IP tới các thiết bị mạng bên trong một công ty có thể sẽ phức tạp, hao tốn thời gian và tác vụ dễ mắc lỗi nếu điều khiển nhân công.

Một giải pháp đối với vấn đề này là sử dụng cấp phát địa chỉ IP động qua DHCP. Vì địa chỉ tới tên được ánh xạ toàn bộ với bất kỳ mạng IP, nó cũng cần thiết để liên kết DNS tới DHCP, việc này được hoàn thành qua DNS động (DDNS). Các cấu hình sử dụng đa máy chủ là cần thiết nếu tường lửa được sử dụng để phân chia mạng thống nhất riêng từ một phần của Internet.

Các thủ tục cấp phát các địa chỉ IP chung, với giới hạn số của các địa chỉ được định nghĩa trong IPv4 nên cần thiết có một giải pháp biến đổi để định tuyến đơn giản trên Internet và sử dụng các địa chỉ IP trên các mạng thống nhất. Phép định tuyến địa chỉ mạng được thử nghiệm là giải pháp phổ biến cho tổ chức thương mại muốn duy trì không gian địa chỉ IP riêng cho Intranet trong khi vẫn duy trì kết nối với Internet chung. NAT cũng góp phần xây dựng VPN một cách dễ dàng.

CHƯƠNG 15

QUẢN LÝ HIỆU SUẤT

Việc nối mạng nếu không được thực hiện tốt sẽ làm người dùng không biết sử dụng băng thông và làm đầy nó một cách nhanh chóng. Tắc nghẽn mạng dẫn đến tính thống nhất có thể bị phá hủy, luồng lưu lượng có độ ưu tiên cao bị ngăn cản không qua được mạng và các người dùng của mạng cũng như các thiết bị mạng không tự giải quyết được vấn đề này.

Hơn nữa, do kết hợp nhiều kiểu lưu lượng khác nhau, các mạng đa dịch vụ ngày nay có thể thực hiện việc điều khiển các thông báo, các giao tác, dịch vụ âm thanh, hình ảnh, thoại và nhiều thứ khác càng làm cho việc cấp phát băng thông và điều khiển mạng gặp nhiều khó khăn hơn.

Chất lượng mạng và VPN có mối liên kết mật thiết với nhau. Nếu các đường hầm được cấp phát có tính trong suốt đối với người dùng và các ứng dụng, để mọi vị trí trong VPN được xem như một tổ chức mạng lớn, thì các đường hầm có thể không can thiệp được hiện tượng nghẽn cổ chai. Tại cùng một thời điểm, các liên kết này có thể không có cùng băng thông như đã tìm thấy trên mỗi vị trí ở LAN. Vậy cần phải chú ý để đảm bảo chất lượng thích đáng giữa các vị trí của VPN.

Vì các cổng nối bảo mật cho một VPN thường liên kết hai miền băng thông khác nhau - ví dụ giữa LAN (tốc độ cao) và WAN (tốc độ thường thấp hơn) - chúng là những điểm nghẽn mạch đối với luồng lưu lượng mạng và có thể phục vụ như những định vị ảo để điều khiển lưu lượng trên cơ sở ứng dụng hoặc quyền ưu tiên người dùng. Với mục đích này, một vài nhà cung cấp đã tính cả việc hỗ trợ độ ưu tiên lưu lượng và quản lý băng thông bên trong các sản phẩm VPN của họ, hai ví dụ đáng chú ý là Contivity Extranet Switches của Bay Network và Firewall-1 của Check Point Software.

Một số vấn đề đáng quan tâm là nền tảng của chất lượng mạng và các yêu cầu ứng dụng liên quan cũng như các phương thức mà các dịch vụ mạng đưa tới

các khách hàng để khách hàng có thể phân biệt trên nền của ứng dụng này và/hoặc các yêu cầu người dùng. Sau đó chúng ta sẽ nói về việc quản lý mạng dựa trên chính sách như thế nào để có thể sử dụng giúp duy trì điều khiển trên các cấu hình mạng và điều khiển băng thông. Cuối cùng, chương này sẽ thảo luận vai trò của ISP trong việc hỗ trợ chất lượng VPN.

15.1 Hiệu suất mạng

Trước tiên xem xét các thành phần của chất lượng mạng rồi thảo luận phương pháp để có thể quản lý được chất lượng mạng.

Mặc dù băng thông là yếu tố có tính quyết định khi xác định tổng số lượng dữ liệu phải được phân phối bên trong một chu kỳ thời gian xác thực, thời gian chờ ảnh hưởng đến thời gian đáp ứng giữa các client và các máy chủ. Thời gian chờ là thời gian nhỏ nhất trôi qua giữa dữ liệu được yêu cầu và được nhận và có thể bị ảnh hưởng bởi nhiều yếu tố khác bao gồm băng thông, cơ sở hạ tầng của mạng liên kết, công nghệ định tuyến và các giao thức chuyển dịch.

Thời gian chờ của một mạng chịu ảnh hưởng của các yếu tố sau:

1. Trễ truyền (Propagation delay): là thời gian giữ thông tin để truyền đi trên lộ trình của đường truyền. Trễ kiểu này phần lớn được xác định bởi tốc độ của tải trọng và không bị ảnh hưởng trong việc sử dụng công nghệ nối mạng.
2. Trễ truyền dẫn (Transmission delay): là thời gian để gửi gói qua một môi trường đã cho. Trễ truyền dẫn được xác định bởi tốc độ tải trọng và kích thước gói.
3. Trễ xử lý (Processing delay): là thời gian yêu cầu để cho bộ định tuyến xem xét các tuyến, tiêu đề được thay đổi và các tác vụ chuyển mạch khác.

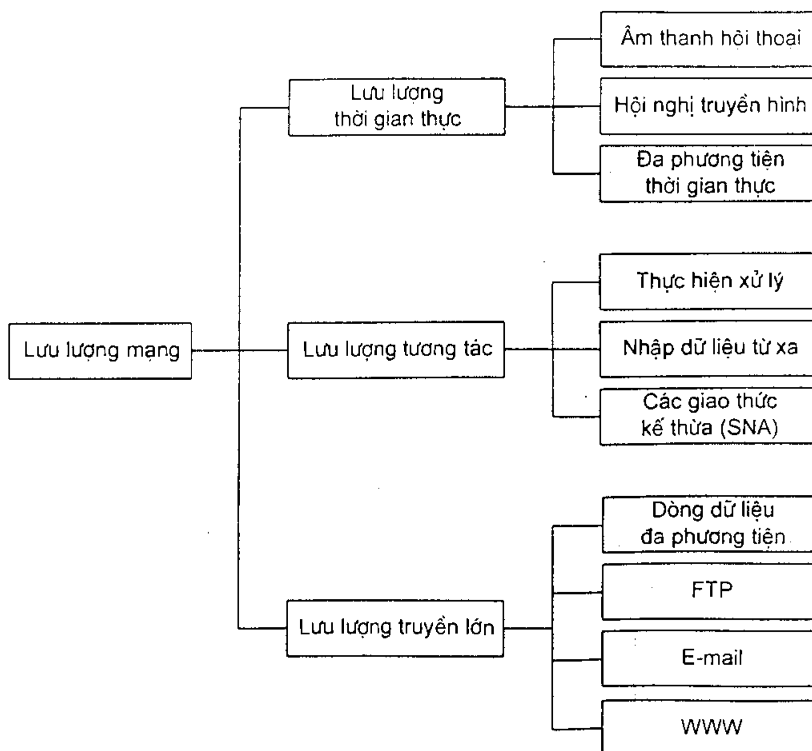
Các yếu tố khác, đó là độ dao động cũng ảnh hưởng tới thời gian thực của lưu lượng mạng. Độ dao động chính là biến hoá của thời gian chờ. Trì hoãn gói bất thường có thể đưa đến hoạt động sai, làm cho các tín hiệu đa phương tiện không thể chấp nhận được.

Với nỗ lực chuyển phát tốt nhất được đưa ra bởi IP thấy rằng các mạng IP xử lý mọi gói một cách độc lập, một nguồn có thể truyền một gói tới một đích mà không cần bất kỳ liên lạc hoặc thoả thuận trước. Hơn nữa, mạng không thông tin để một gói riêng thuộc về một nhóm các gói thích hợp, như khi dịch chuyển một tệp hoặc một dòng video. Mạng sẽ làm việc một cách tốt nhất để phân phát từng gói cách độc lập. Phương pháp này thường đưa đến thời gian chờ và độ dao động đáng kể trong các đường dẫn từ đầu cuối đến đầu cuối nên không tương hợp với

nhiều dữ liệu đưa ra bởi các ứng dụng mới hơn gặp trên các mạng, điều này tuỳ thuộc vào độ trễ và độ dao động được nhận biết, nếu bất kỳ một dữ liệu bị mất. Trễ lớn phù hợp cho các ứng dụng thời gian thực, giống như tương tác đa phương tiện, nó thường không thể chấp nhận các gói truyền lại hoặc có độ trễ trung bình.

Các yêu cầu của những ứng dụng thời gian thực

Sự thay đổi đa dạng của các ứng dụng có thể hoạt động trên nhiều mạng. Phụ thêm vào các ứng dụng truyền dẫn chính yếu như FTP, tin tức trên mạng và e-mail có dải ứng dụng tương tác từ một bộ mô phỏng đầu cuối để yêu cầu nhập vào các lệnh đến điều khiển các đáp ứng ở một host từ xa hoặc sử dụng các trình duyệt Web để xem các trang trên vị trí khác nhau tới các bộ mô phỏng tương tác giữa những người vận hành trong một mạng đa lớp và thậm chí yêu cầu tương tác nhanh hơn cho giao tác xử lý trên thứ tự trực tuyến.



Hình 15.1: Lưu lượng truyền trên mạng

Trong phần trước, những người quản lý mạng có thể dự đoán tương đối chính xác về các dạng lưu lượng của mạng sẽ tốt như thế nào, vì có duy nhất giới hạn về các máy chủ, các cơ sở dữ liệu kế thừa và các tài nguyên mạng khác mà hầu hết các người dùng truy cập. Nhưng, có sự thay đổi đáng kể trong một vài năm qua khi World Wide Web và các ứng dụng mang tính hợp tác đã thay đổi tương

tác giữa những người dùng, cả bên trong và ở giữa các mạng con của mạng liên kết. Tại cùng một thời điểm, các ứng dụng mới khác như dùng dòng đa phương tiện, hội nghị truyền hình và v.v..., đã tăng lưu lượng trên các mạng.

Lưu lượng truyền qua các mạng thương mại tích hợp có thể được nhóm lại trong 3 loại sau: lưu lượng thời gian thực (Real-time traffic), lưu lượng tương tác (Interactive traffic) và lưu lương truyền lớn (bulk transfer traffic) (xem hình 15.1).

Lưu lượng thời gian thực như hội thoại tiếng nói, hội nghị truyền hình và đa phương tiện thời gian thực, yêu cầu thời gian chờ rất ngắn và độ dao động được điều khiển. Một khi các yêu cầu băng thông tối thiểu đã thoả mãn, băng thông sẵn sàng cao hơn có thể mang đến chất lượng tốt nếu các ứng dụng được thiết kế để sử dụng nó.

Lưu lượng tương tác như thực hiện xử lý, nhập dữ liệu từ xa và một vài giao thức kế thừa (ví dụ như SNA), các khoảng thời gian chờ yêu cầu khoảng một giây hoặc ít hơn. Các khoảng thời gian chờ lớn hơn dễ gây ra các trễ xử lý vì những người dùng phải đợi trả lời cho các thông báo của họ trước khi họ có thể tiếp tục thực hiện công việc. Lưu lượng tương tác không yêu cầu băng thông lớn, nên cần thiết phải đáp ứng được các yêu cầu thời gian chờ.

Lưu lượng truyền lớn chấp nhận thời gian chờ mạng, bao gồm các khoảng thời gian chờ một vài giây, nó nhạy hơn thời gian chờ của băng thông sẵn có. Băng thông tăng có thể đưa đến thời gian truyền giảm một cách rõ ràng; tất cả các ứng dụng thuộc loại lưu lượng truyền lớn được thiết kế để sử dụng toàn bộ băng thông sẵn sàng.

Với bước tiến đến việc tương tác đa phương tiện, bây giờ các ứng dụng yêu cầu điều khiển trên chất lượng dịch vụ (QoS) chúng nhận được từ các mạng. Để hỗ trợ các yêu cầu về băng thông và thời gian chờ khác nhau của đa phương tiện và các ứng dụng thời gian thực khác, mạng có thể sử dụng các thông số QoS để chấp nhận lưu lượng mạng và quyền ưu tiên của ứng dụng, nó có liên quan đến các yêu cầu QoS khác ở các ứng dụng khác nhau. QoS cung cấp các dịch vụ mạng được phân lớp bởi băng thông, thời gian chờ, độ dao động và tỉ lệ lỗi của chúng.

Tăng việc sử dụng đa phương tiện không phải là lý do duy nhất để phân biệt các dịch vụ phân lớp và điều khiển lưu lượng trên mạng của bạn. Một vài lưu lượng truyền trên mạng có ảnh hưởng lớn đến các ứng dụng. Vậy nó trở nên quan trọng để có thể phân biệt các lớp của lưu lượng mạng và có một hệ thống để phân phối các lớp này trong các phương pháp khác nhau.

15.2 Các phương pháp hỗ trợ phân lớp dịch vụ

Có nhiều phương pháp hỗ trợ cho phân lớp dịch vụ góp phần làm tăng hiệu suất, giảm tắc nghẽn mạng. Có 5 công nghệ chung nhất được đề xướng như sau:

1. Dự phòng quá băng thông mạng.
2. Duy trì băng thông.
3. Quyền ưu tiên lưu lượng.
4. Cấp phát tài nguyên tĩnh.
5. Cấp phát tài nguyên động

Dự phòng quá băng thông mạng không phải là phương pháp chính xác đối với các dịch vụ phân biệt, nhưng nó có thể giúp phân phối đối với tắc nghẽn mạng bởi mạng được phép điều khiển một khối lưu lượng lớn. Nó là giải pháp thích hợp đối với LAN cục bộ. Nhưng, với WAN và các VPN, dự phòng quá băng thông có thể không phải là giải pháp thích hợp có thể tồn tại vì giá băng thông bổ sung cao.

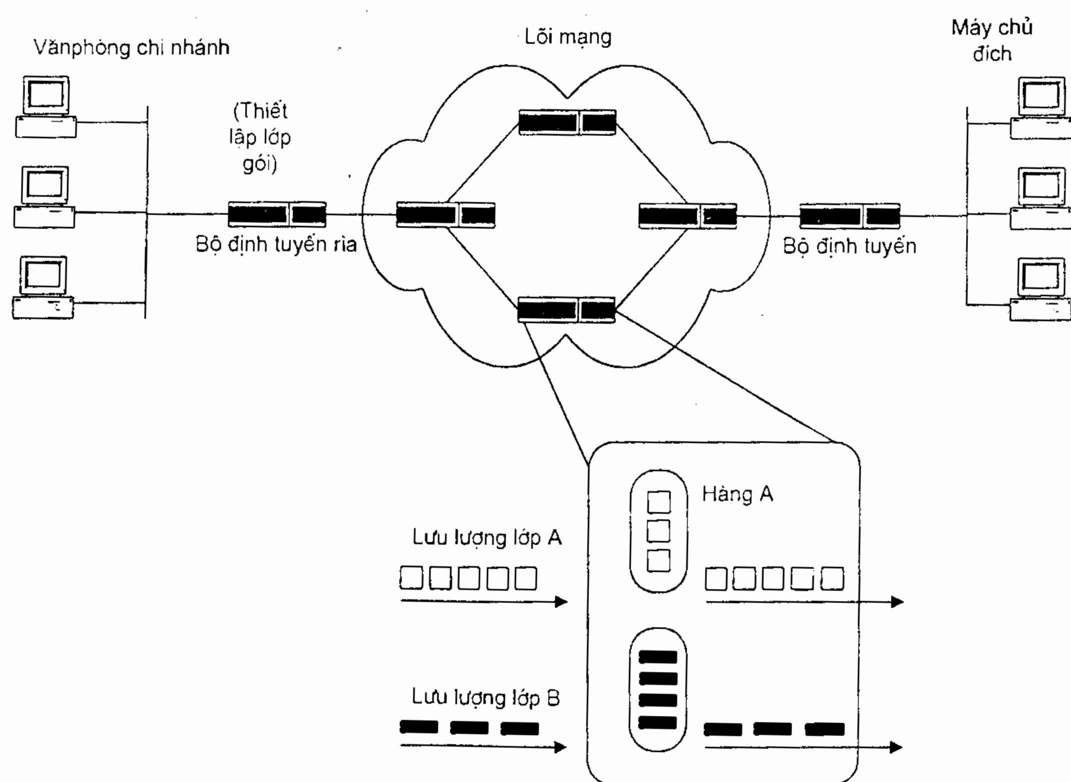
Các công nghệ duy trì băng thông cải tiến toàn bộ chất lượng mạng bởi cố gắng để đảm bảo sử dụng có hiệu quả nhất khả năng sẵn sàng của mạng hơn là phân biệt các dịch vụ. Một vài công nghệ duy trì hiện nay là quảng bá IP (IP multicasting), nén dữ liệu và cung cấp băng thông theo yêu cầu.

IP multicasting giảm tổng số giá trị của lưu lượng trên mạng bởi việc loại bỏ lưu lượng dư thừa đang chuyển tiếp (để chi tiết hơn, xem mục *IP Multicasting* của cuốn "*Hướng dẫn đầy đủ về mạng tổ hợp tương tác*" của John Wiley và Sons năm 1998). Công nghệ thứ hai, nén băng thông, có thể được hoàn thành trong các bộ định tuyến để giảm các yêu cầu băng thông cho một liên kết WAN. Cuối cùng, băng thông theo yêu cầu BOD (bandwidth on demand) có thể sử dụng để cung cấp thêm băng thông khi có nhu cầu bởi việc sử dụng bổ sung các đường truyền điện thoại số hoặc tương tự khi giao tiếp WAN trở nên tắc nghẽn.

Mỗi một phương pháp này có thể không không được áp dụng trong VPN, nhưng chúng được ứng dụng tuỳ theo từng yêu cầu. IP multicasting chỉ làm việc tốt khi dữ liệu đồng thời được truyền tới một số các người nhận. Nếu mỗi phiên di chuyển ngang qua một đường hầm của VPN giữa một client khác và một máy chủ khác thì IP multicasting giúp được ít. Nén băng thông có thể cung cấp hữu ích hơn và một vài nhà cung cấp (cụ thể là VPNet) đã chứa cả việc nén băng thông trong các cổng nối bảo mật của họ để xử lý lưu lượng IPSec. Nhưng, tiết kiệm băng thông có thể không đủ làm thoả mãn các nhu cầu của bạn và nó không xác định được các vấn đề về thời gian chờ. Băng thông theo yêu cầu có thể hữu ích bởi việc cung cấp băng thông nhiều hơn nhu cầu, nhưng thêm các liên kết có thể gây

ra các vấn đề cấu hình trên VPN hoặc không thể giảm giá cung cấp đủ băng thông (hoặc thời gian chờ) cho các nhu cầu của bạn.

Quyền ưu tiên lưu lượng hoặc phân lớp dịch vụ CoS (Class of service) đơn giản nhưng lại công cụ hữu ích để cung cấp các dịch vụ phân biệt. Các bộ định tuyến có thể phân biệt giữa các lớp dịch vụ tuỳ theo trường quyền ưu tiên trong tiêu đề mỗi gói (trường kiểu dịch vụ của IPv4 hoặc TOS). Phương thức này đưa ra một số nhỏ cố định các lớp dịch vụ và chỉ bảo đảm để các gói với quyền ưu tiên cao hơn, đạt được dịch vụ tốt hơn và các gói với quyền ưu tiên thấp hơn. Vì không có điều khiển nhập nên không có cơ chế thích hợp để ngăn chặn quá tải ở các lớp.



Hình 15.2: Hoạt động của phân lớp dịch vụ

Để cải tiến dựa trên hỗ trợ phân lớp dịch vụ, các nhà cung cấp sản phẩm nối mạng chính như Cisco và 3Com đưa vào chương trình điều khiển nhập tại các bộ định tuyến biên (các bộ định tuyến để giao tiếp giữa một LAN, giống như một nhánh LAN của cơ quan và lõi mạng, như Internet hoặc mạng thống nhất chính). Sử dụng các bộ định tuyến biên này để điều chỉnh các cơ chế hoặc các nguyên tắc, để chỉ định lưu lượng tới các lớp trước khi lưu lượng được hướng tới lõi mạng (xem hình 15.2). Các bộ định tuyến trong lõi mạng sử dụng một giải thuật biến đổi để xử

lý các lớp lưu lượng, mỗi lớp có một hàng riêng. Một giải thuật chung để xử lý các hàng là gọi WFQ (Weighted Fair Queueing) cấm luồng lớn, các gói lớn làm hao tốn số lượng lớn băng thông, do vậy có thể duy trì các luồng nhỏ hơn đang được truyền. Bởi vì phân lớp dịch vu được hoàn thành tại các bộ định tuyến biên, đồng thời các bộ định tuyến này có thể là các cổng nối bảo mật cho VPN nên cho phép bạn phối hợp điều khiển VPN và điều khiển lưu lượng tại cùng một điểm.

Nhưng, nếu các lớp sử dụng quyền ưu tiên lưu lượng không đáp ứng được nhu cầu và bạn chọn lọc việc cấp phát các tài nguyên mạng giữa các ứng dụng thời gian thực và thời gian không thực, khi đó bạn có hai lựa chọn. Bạn có thể cấp phát tĩnh các tài nguyên hoặc bạn có thể cho phép các nguồn tài nguyên được cấp phát động.

Cấp phát tài nguyên tĩnh cho phép bạn đặt trước một phần trong số lưu lượng của mạng cho một kiểu lưu lượng chi tiết, thường dựa trên nền giao thức, ứng dụng hoặc người dùng. Cụ thể, trong nhiều mạng thương mại, các bộ định tuyến thường cấu hình để dành hết lưu lượng hiệu dụng cho lưu lượng SNA để thích hợp các yêu cầu của các giao tác dữ liệu kế thừa. Khi lưu lượng được cấp phát cho một ứng dụng hoặc một giao thức đặc biệt, lưu lượng sẽ đủ lớn để thoả mãn các yêu cầu của tất cả lưu lượng của kiểu đó. Nếu không, lưu lượng lớn hơn mức lưu lượng được cấp sẽ có thể bị trễ và\hoặc chọn để loại bỏ. Nếu dung lượng được cấp không được sử dụng, nó ngẫu nhiên dành cho lưu lượng khác để sử dụng phần băng thông còn lại.

Cuối cùng, chúng ta nói đến việc cấp phát tài nguyên động. Đây là phương pháp thu hút phần lớn sự chú ý và nỗ lực của các kỹ sư Internet để có được các dịch vụ tích hợp và giao thức đặt trước tài nguyên RSVP (Resource Reservation Protocol) (xem chi tiết hơn trong phần *QoS và các phương pháp cung cấp QoS trên mạng IP, ATM và Frame Relay*, trong cuốn *"Chất lượng dịch vụ"* (Quality of Service) của Paul Ferguson & Geof Huston; *"Giải phóng QoS trên Internet và trong các mạng thống nhất"* của John Wiley & Sons, Inc, 1998).

Đoán trước biến đổi của các dịch vụ và các ứng dụng thời gian thực có thể được sử dụng trên các mạng IP, IETF thiết lập nhóm làm việc các dịch vụ tích hợp (INTSERV) để thiết kế tập các mở rộng đến mô hình giao phát mạnh nhất hiện nay sử dụng trên Internet. Khung làm việc này là kiến trúc các dịch vụ mạng tích hợp, cung cấp điều khiển đặc biệt cho các kiểu xác thực của các luồng lưu lượng và bao gồm một cơ chế cho các ứng dụng chọn giữa nhiều mức của các dịch vụ phân phối đối với lưu lượng của chúng. Chỉ thị cơ sở của kiến trúc các dịch vụ tích hợp là các tài nguyên mạng đó phải được điều khiển trong lệnh để phân phối QoS, nó yêu cầu nhập vào điều khiển, do đó, cần phải có một phương pháp đặt trước các tài nguyên.

Nhóm làm việc các dịch vụ tích hợp định nghiã một vài lớp dịch vụ đó, nếu hỗ trợ bởi các bộ định tuyến, có thể cung cấp luồng dữ liệu cùng với uỷ thác QoS xác thực. Điều đó tương phản với lưu lượng không nhận dịch vụ uỷ thác từ một bộ định tuyến và làm việc với bất kỳ các tài nguyên sẵn sàng. Mức QoS cung cấp bởi các lớp CoS nâng cao này là chương trình có thể trên mỗi luồng cơ sở tuỳ theo các yêu cầu từ các ứng dụng cuối. Các yêu cầu này có thể được đưa đến các bộ định tuyến bởi các thủ tục quản lý mạng hoặc sử dụng một giao thức đặt trước như RSVP. Các yêu cầu chỉ thị mức của các tài nguyên (băng thông, không gian bộ đệm) đó phải được đặt trước theo vận chuyển chương trình truyền điều đó phải được thiết lập trong các bộ định tuyến để cung cấp yêu cầu uỷ thác từ đầu cuối đến đầu cuối cho luồng dữ liệu.

Chuyển phát hiệu quả nhất là đặc điểm đầu tiên và là kiểu phân phối mặc định cho lưu lượng của Internet và không nhận bất kỳ phòng ngừa đặc biệt bên trong kiến trúc các dịch vụ tích hợp. Có hai lớp dịch vụ là dịch vụ đảm bảo (Guaranteed service) và dịch vụ tải điều khiển được (Controlled-Load service) có hình thức rõ ràng bên trong khung làm việc của kiến trúc dịch vụ tích hợp để sử dụng với RSVP.

Dịch vụ tải điều khiển được cung cấp chất lượng dịch vụ tương đương đối với sức tải nặng và nhẹ bên dưới. Một điểm khác quan trọng với dịch vụ tốt nhất của Internet truyền thống là luồng tải điều khiển được đó không giảm giá trị một cách đáng kể khi tải mạng tăng. Ngược lại, một luồng tốt nhất sẽ bị chất lượng dịch vụ ngày càng xấu hơn (trễ lớn hơn và mất gói) khi tải mạng tăng. Dịch vụ tải điều khiển được dành cho các lớp của các ứng dụng đó có thể giảm chắc chắn tổng cung cấp bị trễ và bị mất đến một mức thích hợp, như việc thích nghi các ứng dụng thời gian thực.

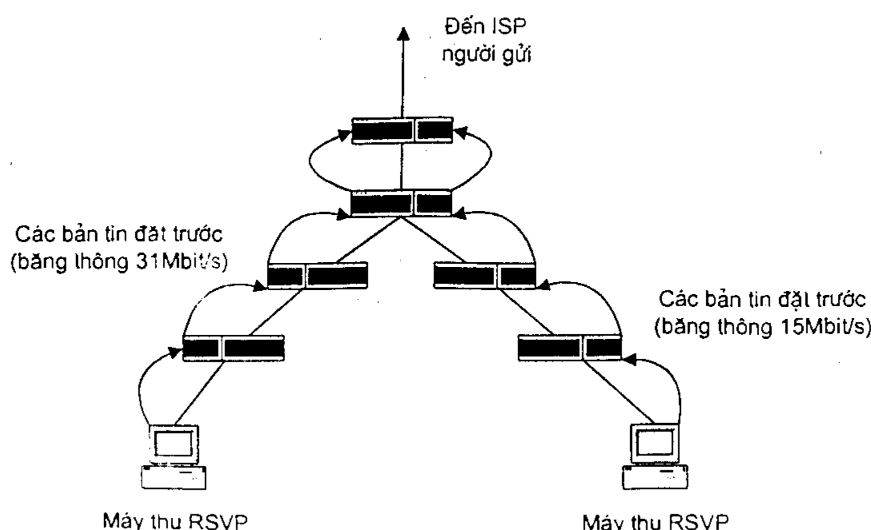
Dịch vụ đảm bảo bảo đảm rằng các gói sẽ đến trong một khoảng thời gian thoả thuận và sẽ bị loại bỏ một cách thích hợp khi hàng tràn, cũng như lưu lượng của luồng ở bên trong phạm vi các thông số lưu lượng đặc biệt của nó. Dịch vụ đảm bảo không điều khiển độ trễ nhỏ hoặc trung bình của lưu lượng và nó không điều khiển hoặc thu nhỏ độ dao động, chỉ điều khiển độ trễ sắp hàng lớn nhất. Nó dành cho các ứng dụng với yêu cầu phân phối thời gian thực nghiêm ngặt giống như các ứng dụng âm thanh và hình ảnh thực để ấn định các bộ đệm phát đi và không chịu nối bất kỳ đơn vị dữ liệu nào đến sau thời gian phát lại của chúng. Dịch vụ đảm bảo được thiết kế để lập địa chỉ hỗ trợ các ứng dụng kế thừa để yêu cầu mô hình phân phối tương tự các mạch truyền tin viễn thông truyền thống.

Trong kiến trúc các dịch vụ tích hợp, có phân chia logic giữa việc điều khiển QoS và thiết kế giao thức để đặt trước tài nguyên, có giao thức đặt trước tài

nguyên RSVP (Resource Reservation Protocol). Đó là vì RSVP có thể sử dụng với trạng thái khác của các dịch vụ QoS và các dịch vụ QoS có thể được thiết kế như một phần của kiến trúc các dịch vụ tích hợp có thể được sử dụng với trạng thái khác của phối hợp được thiết lập. Nếu chúng ta nghĩ RSVP như hệ thống tín hiệu khi đó thông tin điều khiển QoS là nội dung tín hiệu.

RSVP hoạt động ở lớp trên của IP; nó là giao thức điều khiển Internet như IGMP và ICMP, nhưng nó không phải là giao thức định tuyến. Nó sử dụng giao thức định tuyến cơ sở để xác định đích các yêu cầu đặt trước. Khi các đường dẫn định tuyến thay đổi, RSVP chỉnh phần đặt trước của nó tới các đường dẫn mới nếu phần giữ trước ở trong miền. Giao thức RSVP được sử dụng bởi các bộ định tuyến để phân phối các yêu cầu điều khiển QoS đến tất cả nút dọc theo các đường dẫn của các luồng (xem hình 15.3) và tới thiết lập và duy trì trạng thái để cung cấp dịch vụ theo yêu cầu. Sau khi phần đặt trước đã làm được, các bộ định tuyến được RSVP hỗ trợ xác định tuyến và lớp QoS cho mỗi gói vào và bộ lập kế hoạch chuyển tiếp quyết định cho tất cả các gói ra ngoài.

RSVP không triển khai ở vùng rộng; nhiều giao thức chỉ được thừa nhận đến chuẩn IETF kiểm tra cuối năm 1997. Mặc dù một vài bộ định tuyến và các cổng nối bảo mật đã được đặt đúng vị trí với RSVP hỗ trợ, có liên quan về khả năng mở rộng của RSVP. Triển khai của RSVP sẽ tùy thuộc vào hoạt động trên mạng, đó đang là tiến trình của việc định tuyến dựa trên nền QoS và các phương thức truyền bá chính sách mạng tới các bộ định tuyến chính, các bộ định tuyến giữ một phần trong đường RSVP giữa nguồn và đích (một giao thức gọi là chính sách dịch vụ mở chung COPS (Common Open Policy Service) được phát triển cho mục đích sau).



Hình 15.3: Ví dụ minh hoạ RSVP

Lợi ích lớn nhất của RSVP là chính nó thiết lập một cách linh động và dừng hoạt động nhanh chóng các phiên với mức dịch vụ thích hợp: nhờ đó hiệu quả sử dụng băng thông cho lưu lượng kiểu luồng đạt được cao nhất. RSVP không tạo thêm băng thông, nó phân băng thông ra các phần khác nhau. RSVP không làm tăng thêm chất lượng của các ứng dụng dữ liệu tốt nhất; nó cũng không hữu ích đối với lưu lượng Web ngắn hạn vì tổng phí thiết lập các vùng đặt trước.

15.3 Hiệu suất của VPN

Có hai yếu tố chính ảnh hưởng đến hiệu suất của VPN:

1. Tốc độ và độ tin cậy của các đường truyền qua Internet.
2. Hiệu quả xử lý tại các host và các cổng nối bảo mật của VPN.

Như chúng ta đã thảo luận, Internet có thể không cung cấp các thời gian chờ có đảm bảo (độ dao động,...). Các ISP đưa ra các khoảng thời gian chờ có đảm bảo do vậy ngăn lưu lượng đường hầm khách hàng và Internet chung trên mạng đường trục riêng của họ. Các hoạt động này đối với VPN chiếm nhiều thời gian như toàn bộ vị trí của bạn có thể được phục vụ bởi cùng ISP. Không có ISP nào đưa ra các thời gian chờ có đảm bảo cho lưu lượng đi qua nhiều hơn một mạng của ISP, mặc dù vậy các công nghệ và các cơ chế đó vẫn sẽ tồn tại trong một vài năm.

Tất cả những điều đã nói trong chương này trên các phân lớp dịch vụ và QoS, hầu hết các ISP không sẵn sàng đưa ra hỗ trợ đối với các công nghệ này. Các nhà cung cấp sản phẩm mạng đang tích cực đẩy mạnh để tạo ra phần cứng và phần mềm cần thiết sẵn sàng cho các ISP, nhưng ít chấp nhận bất kỳ kỹ thuật cần thiết nào để đưa ra cho các khách hàng các dịch vụ phân lớp.

Nói riêng về chỉ tiêu phí tổn yêu cầu trang bị và lắp đặt các thiết bị, sự thiếu hụt tiêu chuẩn hoá đối với các dịch vụ phân lớp cũng góp phần để ISP bất đắc dĩ chấp nhận các công nghệ đã phác họa. Hiện nay đang xem xét có thực hiện RSVP qua phần lớn các mạng đường trục và Internet chung của ISP hay không thông qua việc so sánh các vấn đề của nó. Giải pháp thích hợp hơn đối với các dịch vụ phân lớp được đưa ra là phương pháp lớp dịch vụ, vì khi xuất hiện nó đã được thử nghiệm bởi các nhà cung cấp khác, như Cisco và 3Com.

MPLS và các ISP

Phương pháp khác, chuyển mạch nhãn đa giao thức MPLS (Multi-Protocol Label Switching) thêm vào lưu lượng IP do vậy nó có thể di chuyển một cách có hiệu quả trên cơ sở hạ tầng chuyển mạch giống như ATM đang được chuẩn hoá bởi IETF và được đưa ra lúc ban đầu bên trong các sản phẩm của Ascend cho các ISP như một phần của đường truyền sản phẩm nhiều VPN của chúng. Bởi vì phần

lớn triển khai MPLS tập trung tại mạng đường trục của ISP, có rất ít khách hàng thương mại sẽ sử dụng MPLS. Chỉ một số ít MPLS hỗ trợ các bộ định tuyến, nhưng điều này sẽ được khắc phục khi giao thức trở thành chuẩn sau năm 1998.

Những gì QoS liên hệ với các dịch vụ ISP đưa ra sẽ có hiệu quả nhất trên các ứng dụng nhạy cảm với trễ theo thời gian. Nếu tất cả lưu lượng VPN đang chuyển dịch là truyền file, duyệt Web và e-mail, khi đó bạn không cần quan tâm đến QoS. Nhưng nếu lưu lượng giao tác, tương tác đa phương tiện và kỹ thuật điện thoại IP đang là một phần lưu lượng của VPN, khi đó bạn cần kiểm tra chất lượng QoS và việc thực hiện QoS của ISP.

Nhưng chỉ quản lý QoS thôi chưa đủ, cần quan tâm đến chất lượng của VPN nữa. Như đã đề cập tại phần đầu của đoạn này, hiệu quả xử lý của VPN là một yếu tố quan trọng. Bạn không muốn các cổng nối bảo mật là các điểm nghẽn mạch đối với lưu lượng mạng thích hợp dẫn tới hiệu quả mã hoá và giải mã các gói kém. Tùy thuộc vào khả năng tính toán của các thiết bị VPN và lưu lượng chúng phải xử lý, bạn có thể quan tâm đến nhiều cổng nối được lắp đặt tại các kết nối nhiều lưu lượng truyền qua và cho phép một vài thủ tục cân bằng tải giữa các cổng nối.

Vì các cổng nối bảo mật là các điểm có ưu thế để tạo các đường hầm VPN nên bạn sẽ có kế hoạch sử dụng chúng để định vị cho việc điều khiển lưu lượng được nhập vào các liên kết VPN. Cụ thể, nếu một cổng nối có thể sử dụng các nguyên tắc lọc cơ sở dựa trên thời gian và ứng dụng, khi đó bạn có thể đặt lọc để đảm bảo rằng lưu lượng quan trọng trong kinh doanh được qua với quyền ưu tiên cao hơn trong nhiều giờ kinh doanh và xem Web có quyền ưu tiên ngang bằng. Dĩ nhiên, thiết lập và quản lý tất cả các nguyên tắc có thể có khó khăn đầu tiên cũng như bạn cố gắng làm cho chúng có hiệu quả qua vô số các vị trí VPN; chúng ta sẽ gặp trong phần 15.4: "Quản lý dựa trên chính sách".

Để sử dụng được phần lớn băng thông do ISP cung cấp, ta không cần chú ý tới các đường hầm được tạo như thế nào và mang lưu lượng gì. Cụ thể, các đường hầm lớp 2 sử dụng L2TP có thể mang lưu lượng ở nhiều phiên. Nhưng, nếu nhiều phiên được dồn vào trong một đường hầm, nó có thể để gói ưu tiên cao hơn trong đường hầm đầu tiên, để có thể phân chia bất kỳ xử lý nhạy tuần tự của các gói giống như nén tiêu đề. Mặc dù các đường hầm nhiều phiên tiện dụng có thể đưa ra, nó tốt cho việc hạn chế các đường hầm tới các phiên đơn hoặc chỉ dồn ít các phiên quyền ưu tiên ngang nhau trong cùng một đường hầm.

Nói riêng về ảnh hưởng lưu lượng được nhận vào như thế nào, các đường hầm VPN của bạn tạo cũng có thể có hiệu quả trong việc triển khai bất kỳ phối hợp QoS mà ISP của bạn đưa ra. Phương pháp đơn giản tác động đến đường hầm

như bọc gói định tuyến chung GRE (Generic Routing Encapsulation) đã được sử dụng trong PPTP, thường ánh xạ bất kỳ trường QoS của các tiêu đề gói tới các trường QoS trong tiêu đề của các gói đường hầm. Nhưng, nếu đường hầm kiểu IPSec được sử dụng, tiêu đề gốc được mã hoá, nếu các cổng nối bảo mật có thể không chuyển dịch thông tin QoS từ các tiêu đề bên trong tới tiêu đề bên ngoài trong các yêu cầu của host bên trong nó đưa ra cho đường hầm, khi đó mạng của ISP sẽ không thể cung cấp bất kỳ chất lượng hỗ trợ cho lưu lượng của đường hầm.

15.4 Quản lý dựa trên chính sách

Trong chương trước chúng ta đã nói về các chính sách trong phạm vi các chính sách bảo mật, bao gồm xác thực và quyền truy cập. Trong phạm vi chương này, quản lý trên cơ sở chính sách có mục tiêu khác - nó sử dụng việc lưu trữ các qui tắc để quản lý băng thông và xác định người dùng có được chất lượng dịch vụ họ yêu cầu như thế nào. Nhưng vì toàn bộ các chính sách trong hoạt động lâu dài đều tập trung trên người dùng hoặc thiết bị, nên điểm nổi bật của việc quản lý mạng dựa trên chính sách là việc sử dụng cơ sở dữ liệu quản lý đơn nhất (phân tán hoặc các loại khác) để điều khiển tất cả các phương tiện của mạng, bao gồm bảo mật, quyền truy cập, các yêu cầu băng thông, v.v...

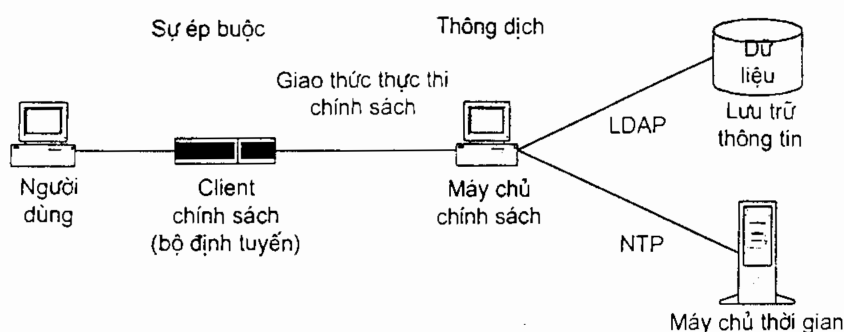
Quản lý mạng trở nên phức tạp hơn không chỉ vì phạm vi các mạng tiến tới kích thước lớn hơn mà còn trở nên phức tạp hơn với các dịch vụ xuất phát trực tuyến và các yêu cầu ứng dụng ngày càng đa dạng. Cần có một phương pháp tốt hơn để quản lý lưu lượng mạng, lập các độ ưu tiên và các yêu cầu băng thông trong một phương pháp tập trung khi mạng tự động trở nên phân tán và kém tập trung hơn.

Như một hình thức của việc quản lý mạng, các nhà cung cấp việc nối mạng chính như Cisco, Bay Network và 3Com đã đang triển khai việc quản lý mạng dựa trên chính sách. Để giúp phân phối đối với tính phức tạp của các mạng, những người quản trị mạng có thể sử dụng việc quản lý mạng dựa trên chính sách nên cần địa chỉ rõ ràng của bất kỳ vùng mở rộng nào của các dịch vụ.

Quản lý mạng dựa trên chính sách đã có trong phần trước khi mà chuyển đổi đã trở nên quan trọng hơn trong các mạng thương mại. Khi chuyển đổi là một phần của mạng thương mại, thường thay thế các bộ định tuyến, người dùng và người quản lý xem xét các phương pháp để đánh giá việc sử dụng các chuyển mạch một cách rõ ràng khi có chuyển đổi, các tài nguyên mạng được phân tán và điều khiển. Nhiều mạng cơ sở trên một lõi hoặc phân cấp các bộ định tuyến không có khả năng ưu tiên lưu lượng mạng trên cơ sở người dùng hoặc độ ưu tiên các ứng dụng. Tương tự, các mạng trên nền ATM có thể đưa ra chất lượng dịch vụ

(QoS) có đảm bảo, nhưng một số ít ứng dụng đã được triển khai để giữ thuận tiện của các yêu cầu QoS này tại mức trạm làm việc. Và RSVP đã được triển khai để cung cấp các khả năng QoS tương tự tới các mạng trên nền IP là tương đối mới và không phổ biến trong các mạng. Nhưng quản lý dựa trên chính sách đưa ra triển vọng làm việc với các trạng thái khác nhau của các thiết bị mạng làm cho quản lý băng thông và cơ chế nhập vào có hiệu lực đối với lưu lượng ứng dụng dọc theo toàn bộ đường dẫn giữa nguồn và đích.

Nguyên lý căn bản của quản lý dựa trên chính sách là các chính sách dành cho quản lý vận hành mạng được đặt ở mức cao hơn bởi người quản trị mạng và các thiết bị mạng thông minh sử dụng các chính sách này để điều chỉnh các tình huống mạng (xem hình 15.4).



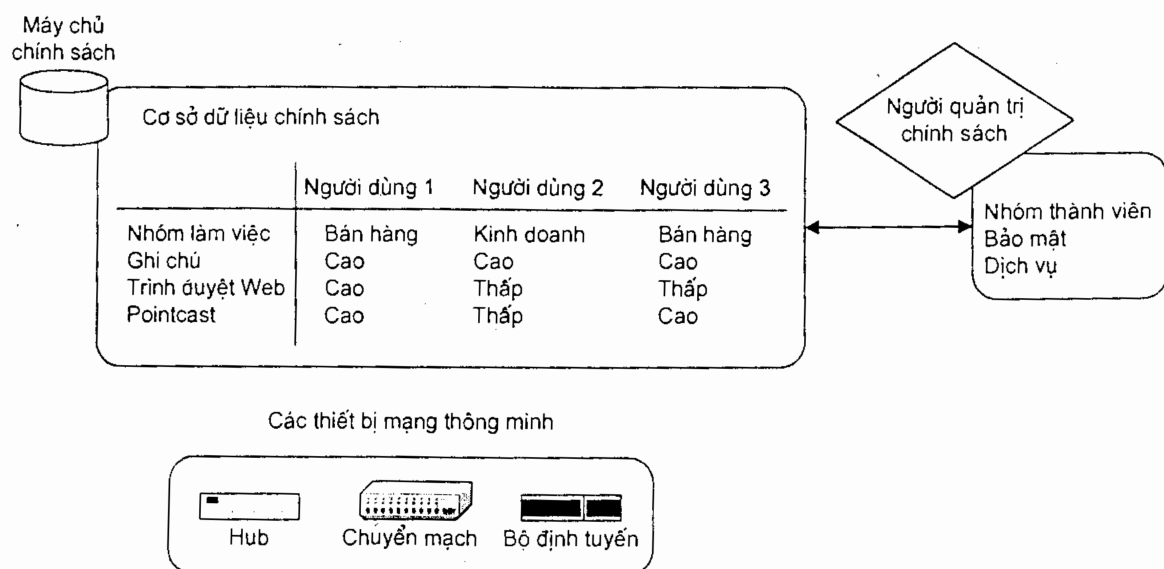
Hình 15.4: Mô hình cơ bản của việc quản lý mạng dựa trên chính sách

Các chính sách quan trọng cho việc điều khiển các yêu cầu ưu tiên được đặt tập trung, thường tại một máy chủ điều hành toàn mạng. Vậy, người quản lý mạng sẽ đặt các chính sách để xác định các người dùng và các ứng dụng đạt được độ ưu tiên cao khi tắc nghẽn làm giảm chất lượng mạng. Khi thiết lập, các cơ chế này có thể tự động được gọi bởi các trạm làm việc, các chuyển mạch và các thiết bị mạng khác khi các tình huống thay đổi trong mạng.

Như ví dụ, xem hình 15.5, ở đây người quản lý mạng thiết lập các quyền ưu tiên cho các ứng dụng trên cơ sở người dùng - người dùng. Các độ ưu tiên này được lưu trong máy chủ điều hành trung tâm, được đặt lại tới mỗi người dùng thích hợp khi trạm làm việc của người dùng bắt đầu khởi tạo và kết nối tới mạng. Sau đó, khi người dùng đặc thù khởi sự ứng dụng mạng đặc trưng trên trạm làm việc, các gói dữ liệu gửi đến mạng được đệm vào với quyền ưu tiên thích hợp và được đặt lại bởi các bộ chuyển mạch tùy theo độ ưu tiên của chúng.

Ma trận hai chiều này của các độ ưu tiên, phân loại bởi người dùng và bởi ứng dụng, cho phép những người dùng khác nhau của mạng có quyền ưu tiên

khác nhau đối với cùng một ứng dụng. Phương pháp này, nó có thể chỉ định một quyền ưu tiên cao cho người quản trị thông tin của công ty CEO sử dụng một ứng dụng SAP trong khi một vài người trong nhóm kỹ thuật hỗ trợ này sẽ có quyền ưu tiên thấp hơn đối với cùng ứng dụng SAP. Một cách tương tự, tất cả cách dùng của PointCast hoặc giống như mở rộng các ứng dụng có thể chỉ định quyền ưu tiên thấp hơn việc sử dụng các ứng dụng SAP. Sau đó cơ sở dữ liệu trên máy chủ điều hành được thiết lập, các bộ định tuyến và các chuyển mạch của mạng có thể điều khiển tự động lưu lượng độ ưu tiên cao nhờ vào lưu lượng quyền ưu tiên thấp hơn trong biến cố tắc nghẽn mạng.



Hình 15.5: Ví dụ việc quản trị mạng dựa trên chính sách

Mặc dù các công ty như 3Com, Bay Network và Cisco đã triển khai thế hệ đầu của các công cụ quản lý chính sách độc quyền, khả năng liên vận hành và các khả năng sẽ được cải tiến qua vài năm tiếp theo nhờ ở nỗ lực của ngành kinh doanh gọi là DEN Initiative (Directory Enable Networking). Công việc này điểm khởi đầu là Cisco và Microsoft, bây giờ đã có hơn 20 nhà cung cấp tham gia và các phương pháp được định nghĩa để sử dụng các thư mục cho việc lưu trữ các tệp cấu hình (profile) của người dùng và thông tin cấu hình thiết bị. Mặc dù nhiều công việc ban đầu đang tập trung trên việc sử dụng thư mục tích cực của Microsoft chính là một phần của NT Server 5.0, các thư mục và các thiết bị sẽ có thể hỏi lẫn nhau và trao đổi thông tin trong việc sử dụng LDAP. Phần mềm quản lý chính sách lúc đó có thể sử dụng tập các nguyên tắc và và lưu trữ chúng trong thư mục DEN; các thiết bị mạng lúc đó có thể làm một cách tự động các quyết

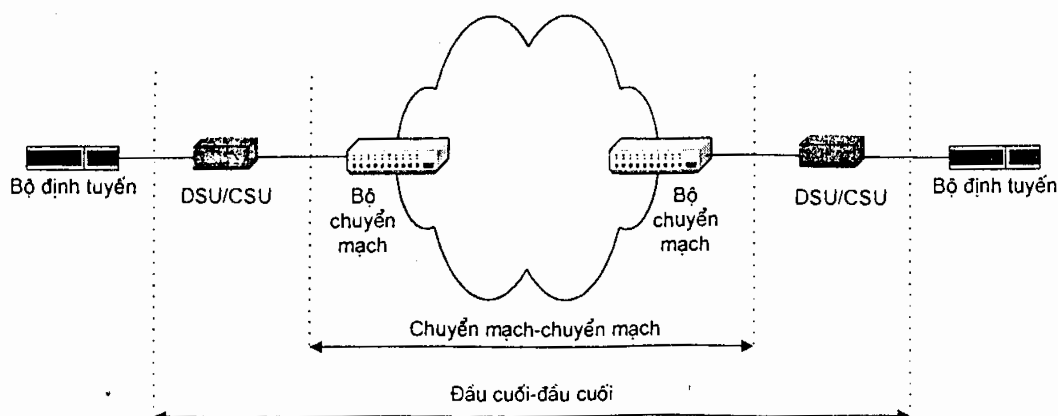
định về băng thông và cấp phát tài nguyên dựa trên các nguyên tắc truyền từ phần mềm chính sách và các tệp cấu hình người dùng lưu trữ trong thư mục DEN.

Bởi vì xu hướng trong quản lý mạng dựa trên chính sách và DEN là tập hợp tất cả mạng và người dùng - liên kết thông tin trong một hệ thống để quản lý tập trung, cả cấu hình của các thiết bị VPN và điều khiển lưu lượng của các liên kết LAN - WAN sẽ được tích hợp trong cùng một hệ thống. Như đã nói, một vài sản phẩm VPN đã được đặt lại với các khả năng LDAP sẽ làm cho tích hợp trong hệ thống quản lý dựa trên chính sách của họ dễ hơn. Nhưng vì cả các hệ thống quản lý dựa trên chính sách và DEN gần đây nỗ lực một cách tương đối nên nó sẽ vẫn có trong một vài năm trước khi có thể triển khai rộng rãi.

15.5 Giám sát hiệu suất ISP và SLA

Chúng ta đã đề cập nhiều chi tiết đến khả năng của ISP và thỏa hiệp mức dịch vụ SLA. Nhớ rằng SLA sẽ được sử dụng để chấp thuận dựa trên những gì là dự định hợp lý của dịch vụ. Có 3 mục cơ bản sẽ đề cập trong mọi SLA: tính sẵn sàng, năng suất và độ trễ.

Giám sát chất lượng của ISP của bạn sẽ làm không chỉ việc đảm bảo rằng các tình huống của SLA của bạn giao được với nhau mà còn xác định VPN của bạn hoạt động như thế nào. Cụ thể, nếu lưu lượng VPN không lấy qua được hoặc bị trễ vì tắc nghẽn tại một cổng nối bảo mật không phải do chất lượng ISP - lúc đó chính bạn phải quan tâm thiết lập một cổng nối có khả năng hơn hoặc cân bằng tải giữa nhiều cổng nối. Nếu một vài liên kết của bạn không sử dụng tải nặng, bạn có thể thỏa thuận một tốc độ chậm hơn cho các liên kết này.



Hình 15.6: Phép đo của SLA

Mặc dù SLA có thể có cơ sở trên 3 mục chúng ta đã đề cập trước đây - tính sẵn sàng, năng suất và độ trễ - những người dùng của bạn đang hoạt động phần

lớn được liên kết với chất lượng của các ứng dụng của họ trên mạng. Bạn nên thường xuyên theo dõi một số các thông số để đo lường chất lượng, như thời gian để tải xuống một tệp hoặc gửi một thông báo.

Bạn giữ lấy vị trí mà phép đo của bạn có thể có ảnh hưởng lớn trên các kết quả đạt được. Phép đo có thể được giữ từ đầu cuối đến đầu cuối hoặc chỉ bên trong một vùng mạng của ISP (xem hình 15.6). Tại chỗ vòng lặp có thể có ảnh hưởng nhiều đến chất lượng mạng, nhưng nó không được để ý trong khi đo chuyển mạch tới chuyển mạch. Các phép đo chất lượng và dàn xếp tranh chấp phải được thực hiện từ đầu cuối đến đầu cuối.

Phương pháp thứ hai là sử dụng một hệ thống đo lường là bộ phận độc lập của mạng bạn đang đo. Yêu cầu thiết bị đo không làm ảnh hưởng đến phía chuyển mạch cũng như kiến trúc bộ định tuyến.

Tổ hợp nhiều công cụ giám sát và thông báo trên dữ liệu từ người đại diện SMNP. Các đại diện SMNP thực hiện chức năng của dữ liệu thời gian thực được tích lũy và phương pháp này thực hiện tốt với các phép đo liên quan băng thông. Phần lớn các bộ định tuyến và các thiết bị mạng khác sẵn sàng đối với các nhà đại diện SMNP để cung cấp phần lớn thông tin cần thiết cho việc giám sát tính sẵn sàng và việc sử dụng.

Các hệ thống giám sát khác kiểm tra vòng các thiết bị sử dụng các giao thức ứng dụng đặc biệt như FTP và HTTP hoặc hệ kiểm tra vòng mức mạng với giao thức thông báo điều khiển Internet - ICMP (Internet Control Message Protocol). Nhưng các hệ thống kiểm tra vòng có thể bao gồm các yếu tố vượt ra ngoài phạm vi hoạt động, điều khiển của các nhà cung cấp dịch vụ (cụ thể, máy chủ Web bị quá tải tại vị trí hợp nhất không thuộc trách nhiệm của ISP của bạn). Một phương pháp tốt sẽ sử dụng hệ kiểm tra vòng ICMP và vị trí thiết bị kiểm tra vòng đóng khít như dịch vụ có thể đang được đo (giao tiếp LAN-WAN trong trường hợp này).

Chấp nhận định nghĩa của các thông số đo và phương pháp đo như thế nào là một tác vụ quan trọng, nhưng đó là một việc không dễ hoàn thành một cách chi tiết bởi vì không có chuẩn hoá các phép đo này giữa các ISP. Mặc dù nó sẽ ở trong khoảng thời gian trước chuẩn bị các phép đo chất lượng mạng IP và sẵn sàng chấp nhận ở trên, kiểm tra hoạt động của nhóm làm việc IETF trên các phép đo chất lượng của nhà cung cấp Internet - IPPM (Internet Provider Performance Metrics) để thấy các nỗ lực trước đây.

Nhiều nhà cung cấp dịch vụ đưa ra dịch vụ có đảm bảo sẽ thường định vị các thiết bị đo tại CPE của bạn. Để đối chiếu lợi ích, bạn thử định vị các thiết bị đo

lường riêng của bạn song song với thiết bị của ISP. ISP đưa ra các kết nối giữa quản lý và môi trường giám sát và khách hàng - các môi trường quản lý của họ, cho phép khách hàng truy cập trực tiếp tới dữ liệu được liên kết tới VPN của họ.

Tổng kết

Trạng thái khác nhau của các ứng dụng mạng có các yêu cầu khác nhau đối với băng thông, thời gian chờ và độ dao động, tính phức tạp và quy hoạch băng thông dự phòng và điều khiển lưu lượng. Nhiều ứng dụng mới như đa phương tiện tương tác và hội nghị truyền hình, hạn chế chặt chẽ hơn thời gian chờ và độ dao động mạng hơn hầu hết các ứng dụng khác.

Các mạng có thể hỗ trợ các ứng dụng nếu chúng được cấu hình cho các dịch vụ phân lớp. Năm phương pháp đưa ra với các dịch vụ phân lớp là dự phòng quá băng thông, duy trì băng thông, quyền ưu tiên lưu lượng (hoặc phân lớp dịch vụ), cấp phát tài nguyên tĩnh và cấp phát tài nguyên động.

Bởi vì các thành phần quan trọng của VPN được định vị tại giao tiếo LAN - WAN, chúng không chỉ là điểm nghẽn mạch cho lưu lượng mạng mà còn đưa ra cơ hội để lưu lượng được điều khiển và các dịch vụ phân lớp. Nhưng, bất kỳ khi nào, ISP đưa ra hỗ trợ riêng của họ cho các dịch vụ phân lớp, chú ý đặc biệt là phải trả công để lưu lượng với độ ưu tiên khác nhau được trộn trong cùng một đường hầm hoặc các tiêu đề gói được mã hoá, điều đó làm tiêu tan phần lớn phối hợp quyền ưu tiên.

Cơ chế quản lý mạng cơ sở là một vùng được triển khai nhanh chóng, hứa hẹn việc thực hiện cấu hình thiết bị và điều khiển tự động lưu lượng dễ dàng hơn. Cuối cùng, điều khiển cấu hình VPN và người dùng sẽ được chứa trong các hệ thống cơ chế quản lý mạng cơ sở.

PHẦN IV

HƯỚNG PHÁT TRIỂN TRONG TƯƠNG LAI

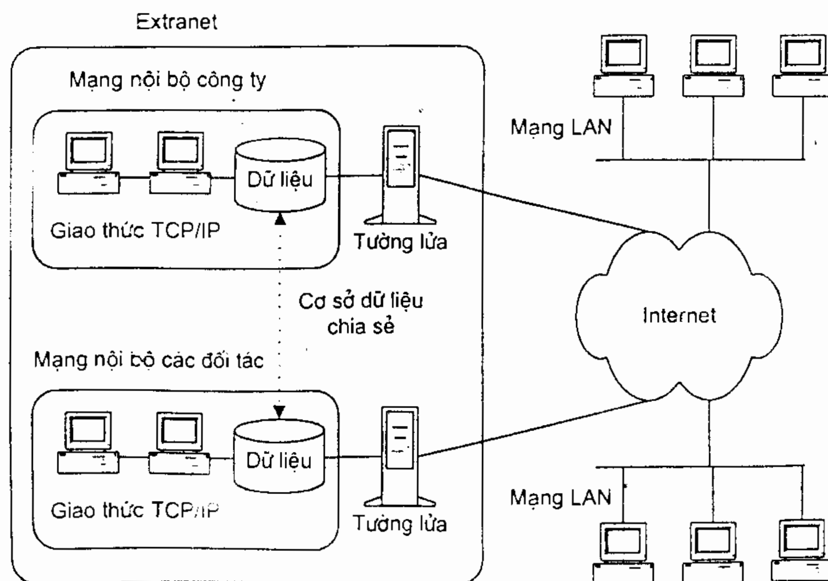
Ngày nay VPN đã vô cùng hữu ích và có phân phối rộng lớn các tiềm năng và sẽ ngày càng hữu ích trong tương lai. Các chuẩn hoá đã được thi hành, điều đó sẽ cải tiến khả năng liên vận hành và quản lý. Chất lượng mạng trên các VPN cũng sẽ được cải thiện, cho phép các liên kết VPN được sử dụng với các ứng dụng mới như hội nghị truyền hình và kỹ thuật điện thoại IP.

Để kiểm tra các sản phẩm có khả năng liên vận hành bạn nên xem ở ICSA cho việc thử khả năng chấp thuận của chúng với chuẩn IPSec và ở ANK cho thông tin có hiệu lực trên các sản phẩm như thế nào để cùng làm việc trong thế giới thực.

CHƯƠNG 16

MỞ RỘNG CÁC VPN ĐẾN EXTRANET

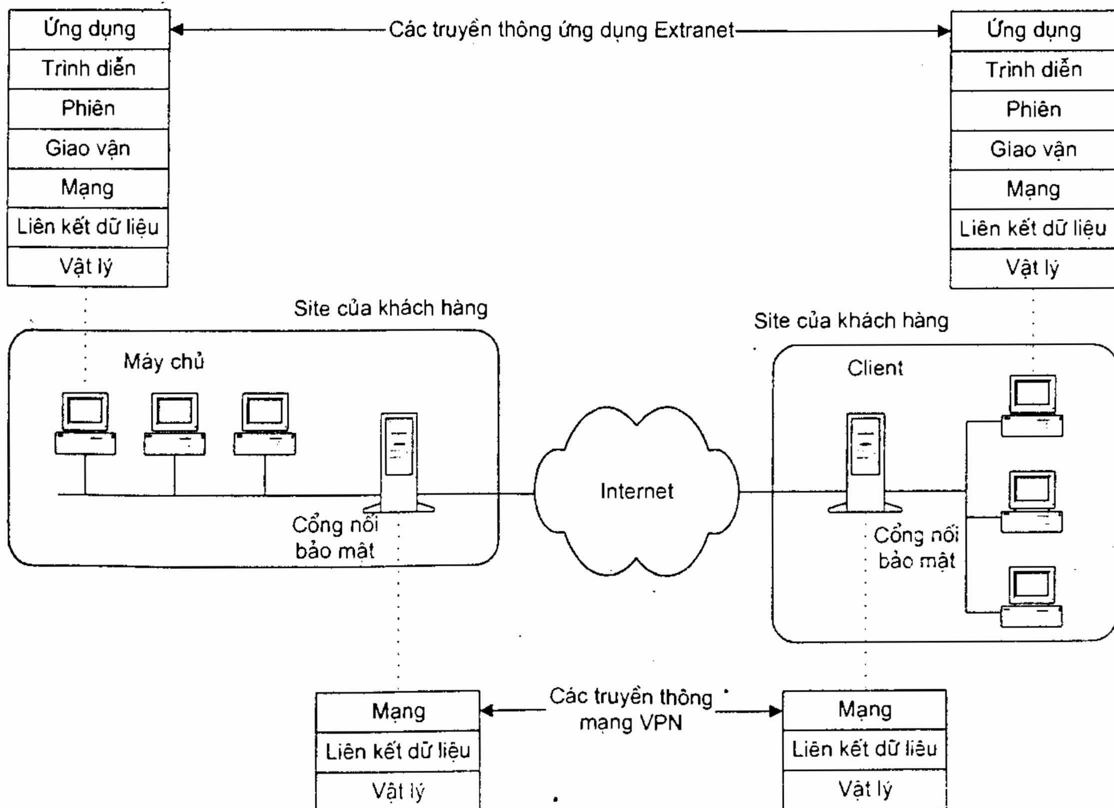
Internet và các mạng TCP/IP khác đã có trên 20 năm nay. Nhưng. chỉ những năm gần đây, Internet mới trở nên thông dụng và các nhà kinh doanh hướng chú ý tới việc sử dụng TCP/IP và Web cho tất cả các kiểu truyền thông; bao hàm này không chỉ liên lạc bên trong các tổ chức thương mại mà còn với các khách hàng, những người cung cấp và các đối tác kinh doanh, cuốn hút của việc sử dụng đồng thời các giao thức và trong nhiều trường hợp cùng ứng dụng để thực hiện nhiều tác vụ và các liên kết khác nhau tới các công ty khác nhau là rất thực tế và tiến bộ.



Hình 16.1: Minh hoạ về các Intranet, Extranet và VPN

Trong thế giới kinh doanh, xu hướng lớn nhất trong các mạng IP là thiết kế lại truyền thông thống nhất xung quanh World Wide Web và Extranet. Thương mại điện tử, phương thức đặc biệt trong việc sử dụng Internet để mua và bán lợi ích và các dịch vụ có rất nhiều tiềm năng và nỗ lực của người tiêu thụ thương mại điện tử đối lập với hoạt động liên doanh, thương mại điện tử kéo theo triển khai của một vài đường dẫn khác. Nỗ lực có triển vọng trong liên doanh thương mại điện tử có lồng vào Extranet, điều đó mở ra nhiều lựa chọn của mạng thống nhất để truy cập bởi đối tác kinh doanh của bạn (xem hình 16.1).

Như chúng ta sẽ thấy trong chương này, Extranet có thể yêu cầu phân phối rộng lớn của tổ chức giữa nhiều việc kinh doanh. Và bởi vì bạn đang cố gắng điều khiển truy cập bên ngoài tới tài nguyên của bạn và có thể cũng muốn bảo mật lưu lượng giữa bạn và các cộng tác của bạn, bạn có thể đã thấy bảo mật quan trọng như thế nào tới hoạt động riêng biệt của Extranet. Nếu bạn cần truyền dẫn bảo mật trong phần bổ sung để điều khiển quyền truy cập người ngoài cuộc, khi đó VPN có thể làm nền tảng tốt cho Extranet của bạn.



Hình 16.2: Các ứng dụng Extranet và các mạng VPN

Một điểm khác nhau giữa Extranet và VPN được tập trung trong sự phát triển của chúng. Cụ thể, Extranet được thúc đẩy hơn bởi nhu cầu cho các ứng dụng kinh doanh chi tiết, xử lý nhanh hơn với các hư hỏng của thiết bị hoặc điều khiển bộ kiểm toán tốt hơn và VPN đã phát triển với nhu cầu để cung cấp liên lạc bảo mật trên Internet chung, không kể đến ứng dụng. Vì khả năng này của VPN nên các ứng dụng bạn dự định cho Extranet có thể đưa vào dễ dàng với kiến trúc của VPN; các ứng dụng Extranet có thể ở lớp trên cùng hệ thống VPN như trong hình 16.2

Bạn không được sử dụng VPN để tạo Extranet: giải quyết đó tùy thuộc trên các yêu cầu bảo mật của các ứng dụng Extranet của bạn. Cụ thể, ban có thể sử dụng SSL/TSL truyền thông bảo mật giữa người duyệt Web của đối tác và một máy chủ Web vừa mới duy trì cho Extranet của bạn. Hoặc các thủ tục EDI giao dịch qua e-mail bảo mật (cụ thể sử dụng S/MIME) có thể đủ cho các yêu cầu của bạn. Nhưng trong chương này sẽ tập trung tìm hiểu xem có thể mở rộng VPN trở thành một Extranet như thế nào.

16.1 Các lý do sử dụng một Extranet

Trước khi thảo luận một số chi tiết trong việc tạo một Extranet từ một VPN, ta nghiên cứu sâu một số vấn đề bên trong các Extranet.

Với nhiều nhà quản lý, các Extranet có nhiều thuận lợi cho việc liên lạc giữa nhiều đối tác kinh doanh. Thứ nhất: các Extranet thường được xây dựng để sử dụng các giao thức TCP/IP, mà giao thức này tạo điều kiện thuận lợi cho việc liên kết được các mạng của hai (hoặc nhiều hơn) công ty. Hơn nữa vì Internet chung cũng sử dụng TCP/IP nên các mạng cộng tác có thể được liên kết lẫn nhau bởi việc sử dụng Internet thay vì tốn chi phí vào việc thiết lập các đường kênh thuê riêng (leased-line) hoặc các liên kết khác.

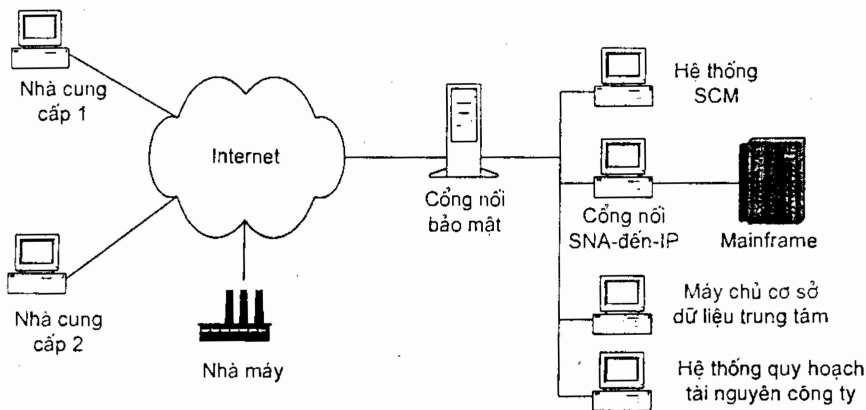
Thứ hai: sử dụng Internet để liên kết các mạng đem đến độ linh động hơn trong các thủ tục và kết thúc các hoạt động ngắn hạn khi cần, điều này ngày càng quan trọng trong thế giới kinh doanh tiến triển nhanh chóng ngày nay. Cụ thể, bạn không thể đợi một tháng hoặc hơn cho việc lắp đặt một kênh thuê riêng. Hoặc, kế hoạch hợp tác giữa bạn và công ty khác có thể chỉ đòi hỏi một lưu lượng nhỏ như vậy sẽ làm giá của kênh thuê riêng quá cao.

Thứ ba: nhiều Extranet luân chuyển xung quanh việc sử dụng World Wide Web, điều này giúp cung cấp giao tiếp người dùng chung tới nhiều ứng dụng qua các ranh giới công ty. Việc sử dụng trình duyệt Web (Web-browsers) đã được phổ biến rộng rãi trong kinh doanh và các công ty đang tiêu thụ phân phối rộng lớn nỗ lực phát triển các ứng dụng để sử dụng Web. Đây không chỉ dễ dàng phân phối phần mềm client mà còn làm cho việc truy cập tới các cơ sở dữ liệu dễ dàng hơn trước đây với các ứng dụng kế thừa.

Một vài đối số cho các Extranet cũng đồng thời cho VPN. Nhưng trong trường hợp kinh doanh có thể khác một chút bởi vì chúng ta đang nói về kinh doanh truyền thông bên ngoài hơn là truyền thông bên trong một Extranet do các VPN hỗ trợ.

Các mục đích kinh doanh của một Extranet luôn thay đổi, nhưng việc liên lạc với các cộng tác tại trung tâm của mỗi Extranet. Nó đòi hỏi loại dữ liệu bạn muốn chứa hoặc chia sẻ, nó có thể kiểm kê các mức, trạng thái các công cụ hủy và chuyển xuống, thị trường dữ liệu, thông tin sản phẩm và bất kỳ loại dữ liệu kinh doanh có thể có.

Extranet được sử dụng phổ thông nhất hiện nay là quản lý dây chuyền (xem hình 16.3). Từ ý tưởng là gom tất cả các công ty vào việc kinh doanh của bạn: cung cấp các thành phẩm, các dịch vụ thiết bị, nhà sản xuất và các đại lý phân phối. Nhiều công việc tự động trong các bước cung cấp dây chuyền qua các ranh giới giữa các công ty có thể dẫn tới việc xử lý sẽ nhanh hơn, cải tiến việc kiểm kê và quản lý nhằm nâng cao hiệu quả trong sản xuất, hỗ trợ khách hàng tốt hơn.



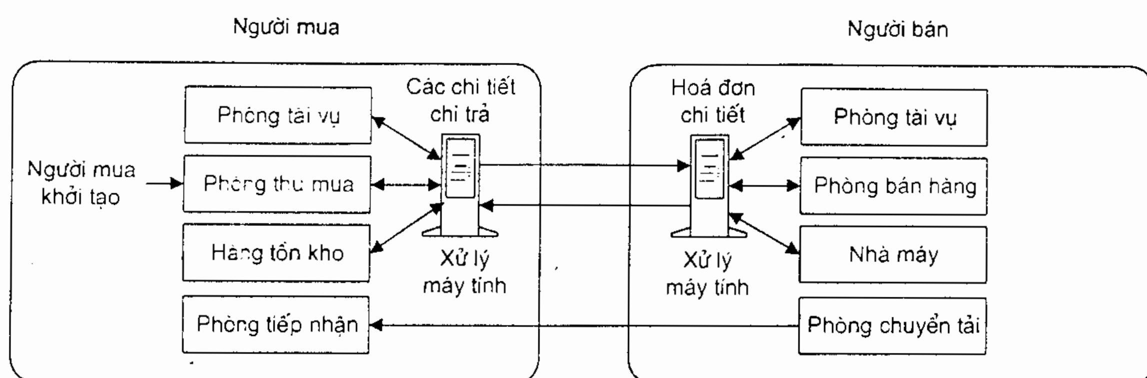
Hình 16.3: Các thành phần của hệ thống cung cấp liên kết

Các Extranet khác có thể không phức tạp, cụ thể, hiện giờ có thể bạn muốn thu được điểm bán dữ liệu mỗi ngày hoặc cung cấp thông tin sản phẩm và cập nhật tập đoàn mới đến chúng qua một máy chủ Web.

Các công ty lớn như Ace Hardware có sử dụng Extranet để cung cấp mạng của những người bán hàng riêng lẻ một cách độc lập truy cập thông tin trước khi nó được lưu trữ trên máy chủ kế thừa và khó truy cập từ bên ngoài. Trong trường hợp Ace, có thể truy cập thông tin mới trên Extranet có chứa các mức kiểm kê tại kho chứa riêng đến những người bán lẻ, các ứng dụng quản lý kiểm kê giúp qui hoạch lại, các công cụ định giá và quản lý biên giúp lưu trữ lợi ích của chủ.

Cần chú ý đến việc xử lý danh mục sản phẩm. Có hai phương pháp xử lý: sử dụng danh mục trực tuyến (on-line catalog) và sử dụng hoán vị dữ liệu điện tử EDI (Electronic Data Interchange).

Danh mục trực tuyến (on-line catalog) đã là một phần chuẩn của thương mại điện tử. Trong phạm vi liên doanh thương mại điện tử, những người cung cấp bắt đầu đưa ra các danh mục trực tuyến theo yêu cầu đến khách hàng, các danh mục (catalog) này có thể có cơ sở từ việc trang bị trước đây hoặc kiểu kinh doanh mới của khách hàng. Khi bắt đầu tiến hành thương mại điện tử chúng dễ cập nhật và sản xuất theo yêu cầu khách hàng. Nếu các danh mục được đưa ra trên một Extranet, truy cập tới các danh mục riêng có thể dễ điều khiển hơn.



Hình 16.4: Luồng thông tin EDI giữa người bán và người mua

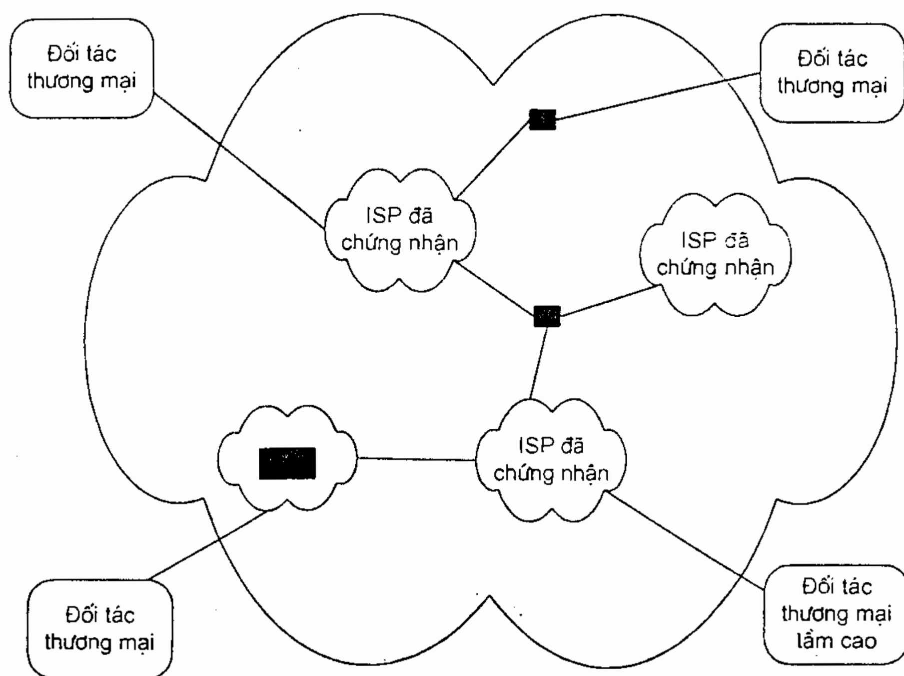
EDI được sử dụng phổ biến bởi các tập đoàn lớn và những người cung cấp vệ tinh làm việc cùng nhau trên một mạng giá trị gia tăng VAN (Value Added Network). Các VAN này đưa ra độ tin cậy và bảo mật cao để khó bị sao chép trên Extranet ở xa. Dữ liệu EDI đưa ra trong các thủ tục được định nghĩa cho các kiểu kinh doanh đặc thù, đặt lại giữa các bên kinh doanh sử dụng e-mail và khi đó trao đổi các định dạng bên trong để cơ sở dữ liệu có thể được sử dụng.

Các tổ chức kinh doanh có thể sử dụng EDI để tự động trao đổi thông tin giữa các ban thống nhất cũng như giữa các công ty. Cụ thể, dữ liệu trên nền EDI có thể trao đổi giữa người mua và các văn phòng nhận để tự động trang bị và xử lý thanh toán (xem hình 16.4).

Vì chi phí hoạt động trên Internet thấp hơn trên VAN, sự quan tâm trong việc sử dụng Internet để truyền dữ liệu EDI đã tăng. Một số nhà cung cấp đưa ra các máy chủ dựa trên Web để thu nhận dữ liệu kinh doanh trong các thủ tục HTML và chuyển tiếp dữ liệu đến các định dạng EDI để truyền trên VAN hoặc Internet. Trong khi đó, IETF đang hoạt động trên một chuẩn đối với thủ tục EDI

kèm theo dữ liệu bên trong các thông báo S/MIME. Để thúc đẩy việc sử dụng EDI trên Internet với nỗ lực mới của công ty W3C (World Wide Web Consortium) thay thế các thủ tục EDI bằng XML (eXtended Markup Language) sẽ làm cho việc cài đặt lại cấu trúc dữ liệu dễ hơn đối với các công ty như việc giành thứ tự bên trong e-mail trên cơ sở IP. Cả EDI và XML trong e-mail trên cơ sở IP và trên Web sẽ làm dễ thay đổi thông tin chúng cần nối kết để điện tử hoá việc kinh doanh cho các cộng tác Extranet.

Kết hợp lớn nhất của các VPN và Extranet là thay đổi mạng tự động ANX (Automotive Network Exchange) làm nhanh chóng có một Extranet với 8000 người cung cấp và 20000 đại lý phân phối được liên kết (hình 16.5). Được tổ chức và quản lý bởi AIAG (Automotive Industry Action Group), Extranet này chứa chứng nhận của người cung cấp dịch vụ IP như việc trình bày rõ khả năng có thể của mỗi phần tử ANX chính nó phải giao nhau trước khi là một phần của Extranet. Extranet dựa trên IPSec để liên lạc trên mạng và sử dụng EDI để thực hiện tự động các nghiệp vụ thương mại giữa các phần tử.



Hình 16.5: Tổng đài mạng tự động

16.2 Điều chỉnh VPN trong Extranet

Bạn đã triển khai một VPN và chính bạn muốn sử dụng các đặc tính bảo mật đã có để tạo một Extranet. Điểm khác biệt chính giữa việc thiết lập VPN và

Extranet là đạt được sự hợp tác của các đối tác kinh doanh. Thậm chí nếu Extranet là ý tưởng của công ty bạn và các ứng dụng triển khai cho Extranet đem lại lợi ích cho các đối tác của bạn, bạn vẫn cần có VPN để tạo Extranet thành công.

Chúng ta không đi chi tiết việc qui hoạch các ứng dụng Extranet hoặc các môi trường triển khai bạn có thể sử dụng cho ứng dụng này. Mối quan tâm chính là Extranet có thể sử dụng các đặc tính của VPN như thế nào, đảm bảo rằng các lý do để lên kế hoạch sử dụng Extranet và kiểu của các ứng dụng đã ổn định.

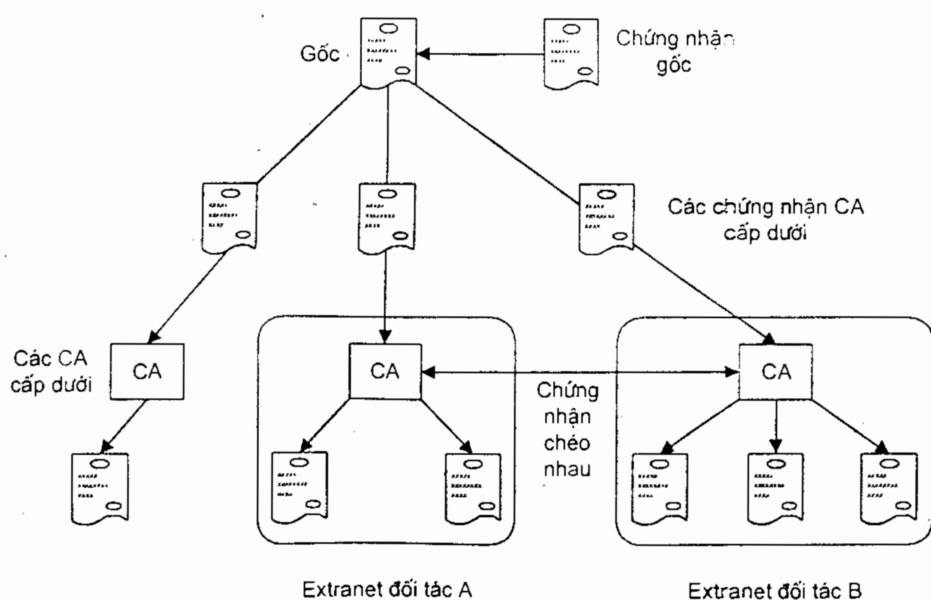
Phần lớn vấn đề bạn sẽ gặp trong việc liên kết các đối tác tới Extranet đều xoay quanh việc tương thích. Có 5 vùng tương thích chính là: thiết lập mạng, các cơ chế bảo mật, các máy chủ xác thực, các giao thức và các chứng nhận điện tử. Việc tương thích này có tầm quan trọng không như nhau và sẽ khác nhau nếu bạn đang thiết lập một Extranet quay số đối lập với việc quy hoạch liên kết hợp nhất các LAN. Cụ thể, việc cung cấp các dịch vụ IP và phần mềm client đến các đối tác nếu sử dụng các kết nối quay số sẽ đơn giản hơn nhiều dù cho IP LAN cần được thiết lập hoặc tái cấu hình và các cổng nối bảo mật được khởi tạo.

Với việc thiết lập mạng, bạn cần biết tại mức tối thiểu nếu bạn đang thiết lập một kết nối LAN-LAN cho dù họ có các bộ định tuyến IP và các liên kết Internet thích hợp nối kết Extranet của bạn. Bạn sẽ mở rộng các VPN đến nhiều vị trí. Tại nơi các đối tác có thiết bị riêng cho cổng nối bảo mật hoặc có cần khởi tạo không? Nếu bạn và các đối tác sử dụng tất cả các địa chỉ IP riêng trên các intranet của bạn, bạn sẽ điều khiển địa chỉ tịnh tiến và các dịch vụ tên giữa các công ty như thế nào?

Các Extranet quay số dễ thiết lập khi nó tương thích mạng. Thậm chí nếu đối tác của bạn không sử dụng IP như giao thức nối mạng chính, việc thiết lập một số máy tính xách tay và để bàn với phần mềm truy cập từ xa, các modem và một tài khoản của ISP đơn giản hơn việc khởi tạo và cấu hình lại một mạng IP và cổng nối bảo mật. Chi phí cũng không đắt.

Các chính sách bảo mật cũng đã được thảo luận nhiều. Nếu bạn đang mở rộng VPN của bạn đến các đối tác Extranet, một số thoả thuận trên các cơ chế bảo mật giữa bạn và các đối tác là cần thiết. Bất kỳ việc gì bạn làm cũng phải bảo mật cho VPN hoặc bảo mật các vị trí bên trong của bạn cũng như của các đối tác. Các công ty nhỏ hơn không có cơ chế bảo mật hoặc họ có thể không hiểu giá trị các tài nguyên được bảo mật. Chi tiết, nếu bạn đang cấp phát các mật khẩu, các thẻ bài bảo mật hoặc các chứng nhận điện tử phải đảm bảo việc bảo mật các đối tác chống lại mất cắp. Một câu hỏi đặt ra là ai có trách nhiệm pháp lý đối với dữ liệu bị mất do mất mật khẩu hoặc thẻ bài không đáng tin tưởng, nhưng sẽ có hợp đồng bảo hiểm hợp pháp cho một vài người.

Các đối tác khác trong Extranet của bạn cũng có thể có phối hợp xác thực khác để sử dụng. Đảm bảo rằng có hai cách thấy đổi dữ liệu giữa các phần tử của Extranet, các hệ thống xác thực sẽ có thể điều khiển được một số người dùng bên ngoài (cụ thể là một số việc làm của các đối tác). Nếu các đối tác khác sử dụng các máy chủ xác thực khác, mọi hệ thống truy cập Extranet sẽ yêu cầu có thể nhiều hơn một phần mềm client. Các đối tác của bạn đã thỏa thuận dựa trên một phương thức chung để xác thực sẽ cấu hình đơn giản và sử dụng Extranet, cũng như việc hỗ trợ giảm giá trong hợp đồng dài hạn (đặc biệt đối với sự trợ giúp tại chỗ). Sử dụng RADIUS, có thể với các máy chủ ủy quyền, là một cách hoạt động vì nhiều hệ thống VPN làm việc với RADIUS và nhiều công ty đang chọn nó để điều khiển truy cập từ xa. Mở rộng RADIUS cũng cho phép nó làm việc với các hệ thống xác thực khác như các thẻ bài SecurID được dùng để giúp RADIUS hợp nhất các hệ thống xác thực.



Hình 16.6: Minh hoạ liên kết các CA với nhau

Cũng có thể sử dụng các chứng nhận điện tử để xác thực những người dùng cũng như các vị trí. Nếu bạn sử dụng các chứng nhận điện tử, kiểm tra độ tương thích của các chưng chỉ - không phải tất cả các chứng nhận đều sử dụng chuẩn X.509v3. Cụ thể, chương trình mã hoá thông dụng đối với e-mail, PGP có định dạng xác thực riêng không tương thích với X.509v3. Bạn cũng cần xác định ai sẽ cấp phát các chứng nhận. Có thể sử dụng một máy chủ xác thực nội bộ hoặc một tác quyền xác thực thương mại cho Extranet cũng như VPN của bạn. Nhưng, nếu

xác thực đang phát hành bởi từng việc kinh doanh tham gia, khi đó bạn cần một phương pháp xác thực CA chéo (xem hình 16.6). Việc đó tương đối dễ cho dù sử dụng CA thương mại của bất kỳ ai vì chúng thường đã qua xác thực. Nếu bạn đang duy trì máy chủ xác thực riêng, khi đó bạn sẽ đăng ký máy chủ xác thực của bạn với một CA bên ngoài hoặc máy chủ xác thực của các đối tác.

Nếu bạn đang tạo một Extranet bởi việc kết hợp nhiều VPN của các đối tác kinh doanh, sẽ có cấp phát khả năng liên vận hành giữa các VPN. IPSec là một bước lớn để giải quyết cấp phát khả năng liên vận hành này, nhưng không mong muốn tất cả các sản phẩm hỗ trợ IPSec ngày nay làm việc cùng nhau một cách tự động. Các chuẩn để quản lý khoá mới mẻ đối với tất cả các nhà cung cấp không trang bị chúng và tất cả các loại hình không làm việc với chúng. Các thủ tục của mỗi đối tác đối với việc quản lý VPN có thể không đồng nhất, vậy bạn sẽ phải xác định cái gì sẽ điều khiển hoạt động ở khắp nơi, đáp ứng bất kỳ các nhu cầu để mỗi VPN làm việc với VPN khác.

Thứ nhất: một vài Extranet được tạo để kết nối các site và dữ liệu chúng làm việc và đưa ra lưu trữ một số nơi. Khi bạn đang thiết kế một hệ thống điều khiển kiểm tra cho một Extranet, nó có thể xác thực với máy chủ xác thực. Một số thành viên của Extranet sẽ quyết định giữ việc đặt lại host của máy chủ để kết nối và duy trì bảo mật.

Thứ hai: là cấp phát quyền quản lý. Để công bằng mỗi thiết bị trên Extranet được quản lý bởi một vài người, kết nối đầu cuối - đầu cuối (end-to-end) ngang qua các ranh giới của công ty. Khi có lỗi xảy ra, có thể khó phát hiện thiết bị bị hư. Để giải quyết điều này, cần phải thiết lập một vài phương thức và thủ tục báo cáo sự cố để cùng liên kết trợ giúp tại chỗ của công ty, do vậy họ có thể hợp tác dựa trên cách giải quyết các vấn đề để chính chúng được nhóm lại trên Extranet.

Bạn có một VPN nội bộ hay một VPN bên ngoài, bạn có thể chọn một ISP duy trì Extranet cho mình. Nhà cung cấp dịch vụ đưa ra các dịchvụ Extranet thường duy trì các máy chủ xác thực giống như bất kỳ máy chủ Web hay các máy chủ cho các ứng dụng khác có thể cần cho Extranet của bạn, bạn nên duy trì việc điều khiển xác thực người dùng và quyền truy cập đối với Extranet bên ngoài. Việc đưa tài nguyên ra ngoài VPN có thể sử dụng giới hạn thật của VPN (cụ thể là máy chủ xác thực) nhưng nó là phương thức tốt nếu bạn xem xét tốt hơn các hệ thống phân chia cho việc bảo mật các mối liên lạc bên trong và cho việc phân phối với các đối tác bên ngoài.

Chính xác với một VPN, bạn nên có kế hoạch lồng Extranet trong phạm vi hoạt động đang bắt đầu với một công trình thử nghiệm. chọn ra một số khách hàng tin cậy và có khả năng vì họ sẽ hiểu được bạn đang muốn thử nghiệm điều gì trong

Extranet. Đảm bảo rằng họ sẵn sàng góp phần khắc phục sự cố và đưa hệ thống trở lại hoạt động. Nếu các ứng dụng Extranet có kèm theo số người dùng khác (cụ thể, cung cấp hoạt động dây chuyền) đảm bảo rằng những người đại diện mỗi lớp người dùng bao gồm cả việc kiểm tra. Trong bất kỳ trường hợp nào để làm được chắc chắn những việc đó thì công ty của bạn phải đáp ứng cho các hoạt động trên mạng riêng của bạn trước khi đưa đến bất kỳ đối tác nào để kiểm tra.

Tổng kết

Extranet thường được thiết lập giữa các đối tác kinh doanh vì đặc thù của các ứng dụng kinh doanh. Vì các VPN lập hệ thống cho các mạng bảo mật và có thể bảo mật bất kỳ loại lưu lượng nào mà không cần quan tâm đến ứng dụng, bạn có thể xây dựng Extranet trên cơ sở của một VPN. Các bước chính trong việc mở rộng một VPN đến một Extranet là chuyển nhượng quyền truy cập các đối tác Extranet đến các tài nguyên đặc biệt bên trong và bổ sung chúng đến các hệ thống xác thực của bạn.

Nhiều hình thức cấp phát tương thích khác sẽ được phát hiện khi bạn triển khai Extranet vì có thể bạn không đảm bảo các hoạt kinh doanh đồng nhất các kiểu mạng. Một số tương thích bạn sẽ phải quyết định xung quanh các chính sách bảo mật, các VPN được tồn tại, các hình thức triển khai xác thực của các đối tác, các khoá và các chứng nhận số sẽ được phân phối như thế nào?

CHƯƠNG 17

ĐỊNH HƯỚNG TƯƠNG LAI

Internet sử dụng các mạng riêng ảo làm cơ hội phát triển lâu dài cho việc kinh doanh, cung ứng cũng như các ISP. Công ty Infonetics Research đã dự đoán thị trường các sản phẩm VPN sẽ đạt tới 12 tỷ USD trong năm 2001. Có nhiều vấn đề kinh doanh đã làm thúc đẩy việc triển khai các VPN một cách rộng rãi như việc giảm giá và những thay đổi trong việc thông tin liên lạc và việc nối mạng, sẽ vẫn duy trì hiệu quả trong một vài năm nữa. Sự thúc đẩy này có thể đưa đến sự phát triển vượt bậc của VPN.

Trong thời gian tới, phát triển nhiều loại hình khác nhau sẽ gây tác động đến các VPN. Trước tiên, ta sẽ đề cập xem các doanh nghiệp sẽ triển khai VPN như thế nào và các ảnh hưởng đối với các ISP trong tương lai. Sau đó ta sẽ xem xét một số vấn đề về trạng thái của các chuẩn, độ bảo mật và các chứng nhận số trước khi chuyển sang việc quản lý VPN. Và cuối cùng là xu hướng phát triển các dòng sản phẩm VPN.

17.1 Triển khai VPN

Một trong các khuynh hướng sử dụng chủ yếu hiện nay đối với các VPN là thay thế các hệ thống truy cập từ xa sử dụng modem và các máy chủ truy cập từ xa đang tồn tại bằng các VPN quay số. Việc sử dụng VPN quay số có thể làm giảm chi phí và khiến cho việc cung cấp cho những người dùng di động thêm mềm dẻo.

Trong thời gian tới các VPN quay số vẫn giữ vị trí quan trọng. Trong thực tế, một số nhà cung cấp và những người quản lý chỉ quan tâm đối với VPN. Việc đa dạng hoá các hình thức dịch vụ mới đã bổ sung giá trị tới các kết nối từ xa bởi việc truy cập được bền vững từ những ISP khác nhau, sẽ tiếp tục làm cho VPN quay số thêm hữu ích, đặc biệt đối với các công ty thương mại đa quốc gia. Khi các giao

thức VPN tiếp tục được chuẩn hoá, thực hiện các dịch vụ khác nhau để cung cấp hỗ trợ khách hàng đối với các giao thức có tính quyết định như L2TP và IPSec.

Khi các công ty ở vào giai đoạn thí điểm kế hoạch VPN của họ, người quản lý sẽ xem xét các lợi ích cho VPN của họ. Khi thoại qua IP (Voice over IP) hay kỹ thuật điện thoại IP (IP telephony) bắt đầu được chú ý, do giảm thiểu được chi phí vì sử dụng đường truyền công cộng như Internet thay cho sử dụng tuyến điện thoại quốc tế, ý tưởng kết hợp tiếng nói và dữ liệu nối qua mạng IP sẽ trở nên có tính khả thi cao. Một vài lưu ý trong việc cung cấp các thời gian trễ chính xác cho thoại có thể được yêu cầu nhưng nhiều đề nghị của ISP là (hoặc sẽ là) phù hợp đối với ứng dụng này. Một lợi ích khác như ứng dụng hội nghị truyền hình bảo mật (secure video conference), nhưng ứng dụng này có thể đòi hỏi thậm chí khắt khe đối với băng thông và chất lượng dịch vụ (tức là muốn sử dụng dịch vụ này ta phải có băng thông rộng và chất lượng dịch vụ cao). Xu hướng khác có thể điều khiển hỗ trợ vào giao thức VPN là triển khai hộp thư (mailbox) rộng khắp thế giới, trong đó e-mail, fax và gọi điện thoại có thể được nhận và xử lý tất cả trong cùng một ứng dụng duy nhất. Các hãng Lucent/Octel và Nortel đã sẵn sàng cung ứng thế hệ đầu của các hệ thống này và đã triển khai trong một số công ty và các chuẩn đã làm tăng tính dễ sử dụng đối với việc truyền fax và các thông báo điện thoại (phone message) sử dụng e-mail đang được hoàn thành, điều đó sẽ giúp các hệ thống liên vận hành dễ hơn. Các thủ tục khác nhau này truyền được thông tin qua các mạng dữ liệu nên dễ dàng bảo mật chúng với một VPN.

Một số công ty cũng bàn bạc về việc triển khai các VPN bên trong, đây là các mạng riêng cục bộ tổ chức xung quanh một văn phòng hoặc một toà nhà, thiết kế để hạn chế truy cập và duy trì liên lạc bảo mật dựa trên sự xem xét bên trong. Nhiều chuyên gia bảo mật đã chỉ ra rằng xâm phạm bảo mật do nguyên nhân bên trong gây ra hậu quả lớn hơn bất kỳ nguyên nhân riêng lẻ khác. Một cách luân phiên, khi mã hoá trên cơ sở host và xác thực trở nên rộng khắp, các kênh riêng có thể được thiết lập giữa các bộ phận của ban để liên lạc bảo mật bên trong tổ chức thương mại.

17.2 Quản lý VPN

Trong vài năm tới, quản trị VPN sẽ trở thành một trong những mối quan tâm lớn nhất như các chuẩn và các hệ thống liên quan. Các VPN liên mạng LAN (LAN-to-LAN VPN) sẽ trở nên dễ quản lý hơn vì phần lớn các tiến trình xử lý trên VPN hoàn toàn có tính trong suốt đối với các người dùng đầu cuối và quản lý khoá phần lớn sẽ thực hiện dựa trên tất cả các vị trí trên mạng thay vì trên một vị trí độc lập nào đó. Dĩ nhiên, việc tăng thêm nhiều người dùng sẽ đòi hỏi phải có các hệ thống xác thực và hệ thống quản lý khoá mạnh hơn.

Do IKE hiện tại chỉ được xem như một chuẩn quản lý khoá cho việc sử dụng IPSec, nhiều công ty đã dành nhiều thời gian cho việc nỗ lực khắc phục các chướng ngại giữa các sản phẩm của họ nhằm làm tăng khả năng liên điều khiển trên toàn mạng.

Như chúng ta đã thảo luận phần trước, việc quản lý các chứng nhận điện tử được cải thiện hơn. Việc điều khiển tối ưu cho các chứng nhận điện tử và việc phân phối các chứng nhận này với nhau sẽ được phát triển trong vài năm tới như nhiều doanh nghiệp đã thực hiện PKI cho cả các mục đích sử dụng trong mạng cũng như ngoài mạng.

Một dòng sản phẩm mới dựa trên việc quản lý mạng dựa trên chính sách sẽ làm cho việc quản lý VPN cũng như các mạng nguyên thủy khác trở nên dễ dàng hơn. Nhưng việc quản lý mạng dựa trên chính sách vẫn còn là một thị trường rất non trẻ và nhiều nhà cung cấp chính hãng kể từ năm 1998 mới bắt đầu áp dụng cơ chế này cho các sản phẩm của họ. Và chắc có lẽ vài năm nữa tất cả các thiết bị cho VPN mới sử dụng cơ chế này.

Nhiều hệ thống quản trị dựa trên chính sách sẽ phụ thuộc vào việc khởi động các mạng kích hoạt thư mục DEN (Directory Enabled Networks). Điều này có nghĩa là LDAP sẽ đóng vai trò liên kết giữa các thiết bị và các danh mục. Do các tệp cấu hình của người dùng, cấu hình của thiết bị và dự phòng băng thông có thể được kết thành trong các khung làm việc của DEN, ta có thể thúc đẩy việc triển khai DEN trong mạng của mình bằng cách tìm mua những thiết bị nào có hỗ trợ LDAP.

17.3 Các ISP và Internet

ISP sẽ tiếp tục giữ vai trò quyết định trong sự phát triển của VPN. Họ có rất ít lợi ích nếu họ chỉ thực hiện dịch vụ truyền và họ đang đứng trước một cơ hội kinh doanh lớn hơn nếu họ có thể đưa ra các dịch vụ giá trị gia tăng (value-added service). Trong một vài trường hợp, điều này đơn giản như việc đưa ra các kết nối với thời gian trễ giảm. Nhưng, ISP mong đợi vượt xa điều này và đưa ra các dịch vụ phân biệt xác thực, có thể sử dụng công nghệ phân lớp dịch vụ (Cisco và 3Com đã đưa ra các sản phẩm này) hoặc chuyển mạch nhãn đa giao thức MPLS (Multi-protocol Label Switching), giao thức này đang được IETF chuẩn hoá.

Mặc dù IPSec là một giao thức định đường hầm kết nối site-site được dùng phổ biến và không cần bất cứ sự can thiệp nào của ISP nhưng cả hai giao thức PPTP và L2TP cũng hỗ trợ cho ISP những lợi điểm trong việc cung cấp những dịch vụ giá trị gia tăng cho VPN.

17.4 Bảo mật và các chứng nhận điện tử

Trong lúc các công ty đang thực hiện các biện pháp nhằm sát nhập các giải thuật mật mã đã có vào trong những sản phẩm của họ thì các nhà khoa học không ngừng tìm tòi, phát minh ra những giải thuật mới hiệu quả hơn nhằm làm cho việc thông tin liên lạc được nhanh chóng và khó bị tấn công hơn. Giải thuật mới nhất đang được thử nghiệm và đã được một số sản phẩm thương mại hỗ trợ là ECC (tạm dịch là kỹ thuật mật mã đường vòng). Nếu ECC ngày càng được sử dụng rộng rãi và nếu như phân tích mã hoá được đáp ứng đủ mạnh thì IETF sẽ dùng giải thuật này chung với IPSec. Chính phủ Mỹ cũng đang xem xét việc thay thế DES (giải thuật mã hoá) đang sử dụng bằng những giải thuật mã hoá mới bảo mật hơn trong thế kỷ 21 này.

Một trong những thị trường phát triển hiện tại cho các biện pháp bảo mật hiện nay đều xoay quanh việc sử dụng các chứng nhận điện tử. Có nhiều sản phẩm đang được phát triển để sử dụng các chứng nhận điện tử cho việc xác thực người dùng và những sản phẩm này sẽ được tích hợp thực sự vào trong các hệ thống VPN. Một nhân tố khiến cho việc tích hợp các chứng nhận điện tử trở nên dễ dàng hơn là việc sử dụng các danh mục tương thích LDAP. Các danh mục X.500 và LDAP có thể được sử dụng để lưu giữ các chứng nhận và hiện nay LDAP ngày càng được sử dụng phổ biến hơn và đóng vai trò như một phương pháp dùng để truy cập các chứng nhận trên và các thông tin liên quan đến các người dùng.

Như chúng ta đã từng thảo luận trong chương 13 "Quản lý bảo mật", một số công ty còn dùng đến các thẻ thông minh (smart card) trong việc truyền các chứng nhận điện tử. Mặc dù các thẻ bảo mật khác dựa trên card vẫn còn được sử dụng trong thị trường, nhưng sự phát triển của các chứng nhận điện tử và những nền tảng danh mục dựa trên LDAP sẽ thực sự chi phối việc sử dụng các chứng nhận dựa trên card trong quá khứ.

Tuy nhiên sự phát triển của các chứng nhận điện tử vẫn còn gặp những vướng mắc trở ngại bởi các nền tảng khoá công cộng hiện tại (PKI). Các tiến trình hiện thời dùng để phân phối và kiểm tra các danh sách hủy bỏ chứng nhận thì vừa bất tiện vừa chậm chạp và ít thích hợp với các mục đích sử dụng trong VPN và các thư điện tử bảo mật. Người ta đã dùng một giải pháp để khắc phục vấn đề trên là sẽ triển khai giao thức trạng thái chứng nhận trực tuyến OCSP (On-line Certificate Status Protocol) sau khi giao thức này được công nhận là một chuẩn.

17.5 Hướng phát triển của các sản phẩm

Ngày nay đa số các nhà sản xuất sẽ hướng tới việc tích hợp nhiều dịch vụ vào trong cùng một sản phẩm duy nhất, làm tăng khó khăn trong việc cài đặt, cấu hình và bảo dưỡng toàn bộ các thành phần trong VPN. Cách tốt nhất để có một giải pháp tích hợp thực sự tốt là mở rộng VPN đến một ISP đạt tiêu chuẩn. Tuy nhiên, các giải pháp tích hợp ngoài ra sẽ trở nên tương thích giữa các nhà sản xuất, việc cung cấp IPSec, việc quản lý khoá, LDAP và quản lý mạng đang được hội tụ trong các chuẩn.

Người ta đã dùng một giải pháp tích hợp dưới dạng một hộp bảo mật dùng trong các cổng nối bảo mật, tường lửa và các dịch vụ mạng khác sẽ được nhóm lại trong một thiết bị. Và trong một vài năm tới, các sản phẩm sẽ kèm theo nhiều ứng dụng quản lý.

Có nhiều thiết bị tích hợp như trên đang được kết hợp với các dịch vụ mạng khác, bao gồm các dịch vụ như Web hay e-mail, như ta đã từng đề cập, ta phải quyết định sẽ tích hợp tất cả bao nhiêu dịch vụ vào trong một hộp duy nhất. Khi một thiết bị được tích hợp nhiều dịch vụ thì có nghĩa là nó sẽ có độ tin cậy và độ bảo mật cao hơn. Việc phân tán các dịch vụ trong các thiết bị thích hợp cũng như các dịch vụ có thể được quản lý từ một sản phẩm duy nhất.

Các thiết bị VPN bảo mật, nhất là các thiết bị như các hệ thống trọn gói yêu cầu ta chỉ phải thực hiện một ít bước cấu hình, chúng đặc biệt rất thích hợp với các doanh nghiệp nhỏ muốn thiết lập một VPN cho họ. Rõ ràng rằng một số thiết bị mà ta đã liệt kê trong chương 11 "Phần cứng cho VPN" có mục đích chính là hướng về những doanh nghiệp nhỏ. Nếu ta muốn mua sản phẩm nào đó, ta phải đảm bảo rằng sản phẩm này phải có khả năng nâng cấp, mở rộng trong tương lai cũng như phải có tính tương thích với những thiết bị hiện có trên mạng. Việc mua một sản phẩm không có khả năng nâng cấp mở rộng hay không có tính tương thích với các chuẩn hiện tại sẽ làm cho hiệu suất mạng giảm sút, việc quản lý, điều hành, nâng cấp sẽ gặp nhiều khó khăn trong tương lai.

Nhìn chung thị trường VPN là một thị trường luôn luôn biến động, người ta không ngừng phát triển ra những chuẩn mới không chỉ dùng cho việc bảo mật trong VPN mà còn cho cả việc quản lý mạng và những chứng nhận điện tử, tất cả những điều này đã làm cho chúng ta có khả năng thiết kế và triển khai được VPN cho công ty của mình.

Và nếu như muốn biết thêm các thông tin về nhà sản xuất thiết bị cho VPN cũng như các chuẩn cho VPN, chúng ta có thể tham khảo những Website dưới đây:

www.ietf.org/html.charter/aft-charter.html

www.ietf.org/html.charter/Cisco-charter.html

www.ietf.org/html.charter/rsvp-charter.html

www.ietf.org/html.charter/pkix-charter.html

www.ietf.org/html.charter/lsd-charter.html

www.ietf.org/html.charter/dhc-charter.html

www.ietf.org/html.charter/ipsec-charter.html

www.ietf.org/html.charter/nat-charter.html

TÀI LIỆU THAM KHẢO

1. **Building and Managing Virtual Private Networks,**
   Dave kosiur, USA, 1998.
2. **The Internet Solution for Remote Access**
3. **Selecting an Internet Service and VPN Technology,**
   Michael A.Goulde April 1999.
4. **Network Protocol Handbook**
   Matthew G.Naugle, McGraw-Hill, Inc.1994.
5. **Data and Computer Communications**
   William Stallings - 1994
6. **Computer Networks**
   Andrew S.tanenbaum - 1996
7. **Internetworking with TCP/IP**
   Volume1 Prentice-Hall 1991
8. **Local And Metropolitan Area Networks**
   William Stallings, Provided by Telstra 1993
9. **Internetworking**
   Second Edition Mark A.Miller, P.E.1995, Printed in USA
10. **Windows NT Server, Virtual Private Network,**
    White Paper-DRAFT, 98
11. **Access VPN**
    1998 Cisco System
12. **Layer 2 Tunneling Protocol**
    1998 Cisco System

MỤC LỤC